

"十二五"普通高等教育本科国家级规划教材　计算机系列教材

离散数学（第3版）

邓辉文　编著

在线教学版 | 教学资源·练习与测试 互动教学·智能学习





扫一扫
登录在线教学平台

清华大学出版社

“十二五”普通高等教育本科国家级规划教材

计算机系列教材

离散数学

（第3版）

邓辉文　编著

清华大学出版社

北京

内 容 简 介

本书根据 IEEE-CS/ACM Computing Curricula 2005 系统地阐述离散数学的经典内容，渗透初等数论知识. 全书共分 8 章，分别介绍集合、映射与运算，关系，命题逻辑，谓词逻辑，代数结构，图论，几类特殊的图以及组合计数. 本书以集合、映射、运算和关系为主线，使全书内容联系紧密，具有较强的逻辑性. 每节都有精选习题，书后有习题答案及提示. 所用符号尽可能与其他专业课程一致，专业术语均有对应的英文.

本书叙述详尽、通俗易懂、结构严谨、逻辑清晰、便于自学，适合于计算机及相关专业作为一个学期教材(48/72/90 学时)，也可供考研学生及相关专业技术人员参考.

本书配套的《离散数学习题解答(第 3 版)》(ISBN 978-7-302-33113-1)同时由清华大学出版社出版，在出版社网站有本书配套的电子教案 PPT 可供下载. 目前，已编写完成 18 套考试题.

图书在版编目(CIP)数据

离散数学/邓辉文编著. —3 版. —北京：清华大学出版社，2013(2018.1 重印)
计算机系列教材
ISBN 978-7-302-32827-8

Ⅰ. ①离…　Ⅱ. ①邓…　Ⅲ. ①离散数学—高等学校—教材　Ⅳ. O158

中国版本图书馆 CIP 数据核字(2013)第 136644 号

责任编辑：汪汉友
封面设计：常雪影
责任校对：白　蕾
责任印制：刘海龙

出版发行：清华大学出版社
　网　址：http://www.tup.com.cn，http://www.wqbook.com
　地　址：北京清华大学学研大厦 A 座　　**邮　编**：100084
　社 总 机：010-62770175　　**邮　购**：010-62786544
　投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
　质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　销：全国新华书店
开　本：185mm×260mm　　**印　张**：17.75　　**字　数**：432 千字
版　次：2006 年 10 月第 1 版　2014 年 1 月第 3 版　　**印　次**：2018 年 1 月第 10 次印刷
印　数：19001～21000
定　价：29.50 元

产品编号：053595-01

前　言

离散数学是研究离散量的结构及其相互之间关系的学科，它与当今计算机所处理的对象相一致. 离散数学是教育部2009年“高等学校计算机科学与技术专业核心课程教学实施方案”中8门核心课程之一,在专业教学体系中起着重要的基础理论支撑作用.

本教材自出版以来被多所高校选用，已连续多次印刷，2012年荣幸评为首批“十二五”普通高等教育本科国家级规划教材. 根据教育部通知要求，入选教材应继续修订完善,及时补充反映最新知识、技术和成果的内容,与时俱进，在原书的基础之上将初等数论知识融入在第1章和第2章，加强了内容的历史发展和进一步待思考问题的概要说明,并做了如下改动.

(1) 在第1章中加入了数论中的基本内容,如素数、素因数分解、模运算、最大公因数、最小公倍数和欧拉函数等. 同时还给出了常见的证明方法:直接法、举反例法、数学归纳法和反证法等.

(2) 在第2章中,将整数集合 **Z** 上的整除、模同余关系作为 **Z** 上的关系很自然地引入,同时还介绍线性同余方程或线性同余方程组.

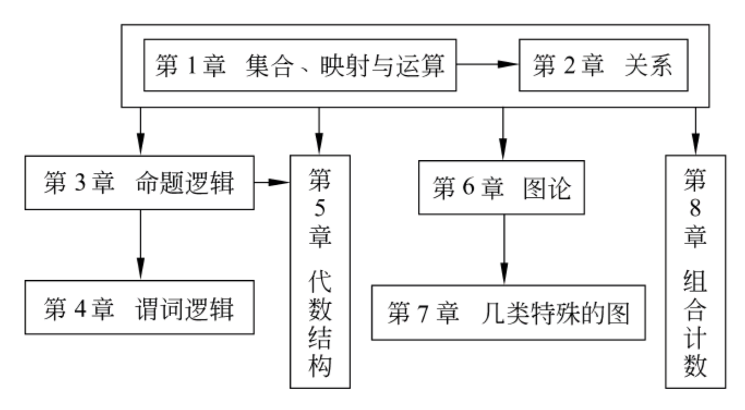
(3) 由于教学时数和多数学校的教学现状,精简了代数结构内容.

(4) 由于组合计数在算法分析和设计中的重要性,组合计数是离散数学课程实施方案中的核心知识单元,属于必学内容,增加“组合计数”一章.

(5) 新增每章小结内容.

(6) 与本教材配套的《离散数学习题解答(第3版)》每章新增自测题及习题解答.

本着离散数学为计算机其他专业课程,如数据结构、操作系统、计算机组成原理、数据库原理、算法设计与分析、编译原理、软件工程、计算机网络及人工智能等的学习提供必要数学基础的原则,同时考虑到大多数高校教学学时数的安排,本书共分8章,分别介绍集合、映射与运算,关系,命题逻辑,谓词逻辑,代数结构,图论以及几类特殊的图和组合计数. 全书以集合、映射、运算和关系为主线,使全书内容联系紧密,具有较强的逻辑性. 每节都有精选习题,书后有习题答案及提示. 各章之间的联系如下图所示：



通过这些内容的学习,以培养学生抽象思维能力(包括符号抽象和计算抽象)、严密的逻辑思维能力以及计算思维(computational thinking)能力,能够将计算机作为认知工具,按计

算机方式求解问题.

本书讲授约需72课时(见下表),根据教学课时以及学生具体情况,对于第4章、第5章和第8章内容可适当删减(第1章最后两节、第2章最后两节也可考虑适当删减),可讲授50学时左右. 适当增加部分内容或加强习题训练,可作为90学时教材使用. 在学习过程中,若能结合本书配套的《离散数学习题解答(第3版)》学习,则能起到举一反三、加深课本内容学习和理解的作用.

学时数安排表

章	节的学时数
1	2+2+2+1+1+1=9
2	2+2+2+1+1+1+2=11
3	1+2+2+2+2+1+1= 11
4	2+1+1+1+1+1=7
5	2+2+2+2=8
6	2+1+1+1+3+1+1=10
7	1+1+2+2+1+1+1+1=10
8	2+2+2=6

在学习过程中,请查阅有关网络教学资源:

(1) Kenneth H. Rosen website: http://www.mhhe.com/rosen.

(2) ArsDigita University: http://aduni.org/courses/discrete/index.php? view=cw.

(3) Harver Mudd College:

http://www.infocobuild.com/education/learn-through-videos/mathematics/discrete-mathematics.html.

(4) MIT(Massachusetts Institute of Technology):

http://ocw.mit.edu/OcwWeb/Electrical-Engineering-and-Computer-Science/6-042JFall-2005/CourseHome/index.htm.

(5) www.izhixue.cn.

教材建设是一项长期的艰苦过程,由于编者水平有限,缺点和疏漏在所难免,恳请大家不吝指正并提出宝贵修改意见,以便不断改进和完善,作者万分感激. 欢迎索取教学用PPT素材和考试用20套考试用套题(huiwend@swu.edu.cn).

感谢重庆市2013年高等学校教学改革研究项目(编号:133013)资助.

编　者

2013年10月

目　　录

第 1 章　集合、映射与运算

集合是现代数学的最基本概念，映射是现代数学的基本概念，运算本质上就是映射，其基本内容在中学已出现. 由于信息科学很多理论研究和应用研究都与集合、映射和运算有关，需要进一步较系统、深入地学习集合、映射和运算的有关内容.

集合、映射、运算和关系是贯穿于本书的一条主线，它们可使离散数学内容不“离散”.

1.1　集合的有关概念

1.1.1　集合

现代数学均建立在集合基础之上，集合已渗透到自然科学以及社会科学的各个研究领域. 集合是表示(离散)对象的数学工具. 在非数值信息的表示及处理中，可以借助于集合去实现数据的表示、删除、插入、排序以及描述数据间的关系，在程序设计、数据结构、数据库和软件工程等课程中会经常用到.

众所周知，集合论创始人德国数学家 G. Cantor(1845—1918)在讨论函数项级数的收敛点问题时定义了集合. 根据 G. Cantor 的朴素集合论观点，**集合**(set)是具有某种特定性质的对象汇集成的一个整体，其中的每一个对象都称为该集合的**元素**(element)，如班上的所有男生就组成一个集合. 我们把一些特定对象看作一个整体就是一个集合，尽管这种理解存在不足之处.

数学上常用一对大括号{ }表示一个整体.

在讨论集合时，应该先指定所讨论的范围，这是避免在集合论中出现某些悖论的最好方法. 所指定的范围本身就是一个集合，称为**全集**(universal set)，有时候称为论域，用 U 表示. 在画文氏(John Venn，1834—1923)图时，用一个矩形框表示，如图 1-1 所示.

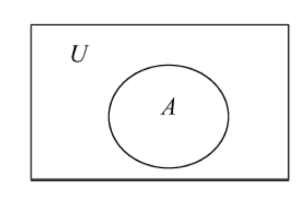


图　1-1

集合通常用大写字母 A,B,C,D 等表示.

给定一个集合，比如 A，对于全集中的任意元素 x，有且只有下述两种情形出现：

(1) 若 x 是 A 中的元素，则称 x **属于** A，记为 $x\in A$；

(2) 若 x 不是 A 中的元素，则称 x **不属于** A，记为 $x\notin A$.

显然，这样的集合 A 有一个明确的边界.

思考　班上的所有高个子同学看作一个整体时是一个**模糊集合**(fuzzy set)[1]，你能想出描述它的方法吗?

常见的数的集合(用正黑体字母表示)有：$\mathbf{N}$ 是自然数集合，包括数 0；$\mathbf{N}^+$ 是正整数集合；$\mathbf{Z}$ 是整数集合(正整数集合也可以记为 $\mathbf{Z}^+$)；$\mathbf{Q}$ 是有理数集合；$\mathbf{R}$ 是实数集合；$\mathbf{C}$ 是复数集合；$\mathbf{Z}_m=\{0, 1, 2, \cdots, m-1\}$.

下面介绍素数集合 $\mathbf{P}$.

对于任意整数 m 和 n，若存在整数 q，使得 $n=qm$，则称 m 为 n 的**因数**(divisor)，又称 m

整除(divides)n 或 n 被 m 整除,记为 $m|n$(与中学要求 $m \neq 0$ 不同). 于是,6 和 -6 的因数有 1, -1, 2, -2, 3, -3, 6, -6, 特别地, $2|6$, $-2|6$, $2|-6$, $-2|-6$. 任意整数都是 0 的因数,即对于任意 $m \in \mathbf{Z}$,有 $m|0$. 对于任意正整数 n,用 D_n 表示 n 的所有正因数组成的集合,于是 $D_{12} = \{1, 2, 3, 4, 6, 12\}$.

对于大于 1 的正整数 p,若 $D_p = \{1, p\}$,即 p 的正因数只有 1 和 p,则称 p 为**素数**(prime),否则称 p 为**合数**(composite number). 素数又称为质数. 1 既不是素数也不是合数. 最前面的 10 个素数为 2, 3, 5, 7, 11, 13, 17, 19, 23, 29.

检查一个大于 1 的正整数是否为素数称为素数测试. 素数测试不仅具有重要的理论意义,而且在计算机密码学中具有十分重要的应用价值. 若 n 是合数,则存在 a 和 b 使得 $n = ab$, $1<a<n$, $1<b<n$. 于是 a 和 b 中必有一个小于等于$\sqrt{n}$. 因此,要检查 n 是否为素数,只需要检查 n 是否有一个小于等于$\sqrt{n}$的大于 1 的因数即可. 根据此结论,可以编写一个程序以检验给定的正整数是否为素数.

当 n 为合数时,即 $n=ab$, $1<a<n$, $1<b<n$,有 $1<2^a-1<2^n-1$ 且 $2^n-1=(2^a)^b-1$. 容易验证 $x^m-y^m=(x-y)(x^{m-1}+x^{m-2}y+\cdots+y^{m-1})$,进而 $2^a-1|2^n-1$,因此 2^n-1 是合数. 当 n 为素数时, $2^2-1=3$, $2^3-1=7$, $2^5-1=31$, $2^7-1=127$ 都是素数, $2^{11}-1=2047=23\times 89$ 是合数. 对于素数 p, 2^p-1 称为 Mersenne 数. 到 2016 年为止,美国 Curtis Copper 教授利用 GIMPS(Greatest Internet Prime Mersen Search)分布式计算项目找到了第 49 个 Mersenne 素数是 $2^{74207281}-1$,这个数有 22 338 618 位。读者也可以加入到 Mersenne 素数寻找的行列中(www. mersenne. org/prime. htm),也许会在 15 分钟内成为名人.

表示集合的常用方法有下面几种:

(1) **列举法** 将集合中的元素按一定规律列举出来,元素之间用逗号隔开,如小于 10 的偶自然数组成的集合为$\{0,2,4,6,8\}$,自然数集合 $\mathbf{N}=\{0, 1, 2, 3, \cdots\}$, $\mathbf{Z}=\{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$. 这种表示方法适用于元素个数有限或元素出现的规律性很强(元素可列)的集合.

注意 所有素数组成的集合 **P** 在理论上可用列举法表示(见第 1.6.4 节可数集合),但由于素数有无限多个且尚未找到其出现规律,用列举法表示在实际操作时存在一定困难.

(2) **描述法** 这种方法用得最多,它只需把集合中元素满足的条件描述出来即可,一般形式是$\{x|x$ 满足的条件$\}$. 例如,小于 10 的偶自然数组成的集合可表示为$\{x|x$ 是自然数且 x 是偶数且 x 小于 $10\}$.

鉴于递归(recursive)法在本书后面章节的讨论中要用到,如合式公式(WFF)的定义,更主要的是这种定义方法在研究递归函数、程序设计中函数的递归调用以及算法的递归实现等内容时的重要作用,下面简单介绍递归法,又称为归纳(inductive)法[2].

大家知道,许多现象的变化呈现出前因后果联系,即现象的变化结果与其前面的一个或几个结果密切相关. 常说的"知道他的过去,就知道他的现在;知道他的过去和现在,就知道他的将来",体现的正是递归的思想.

一般来说,如果一个问题可以归结到其前面一个问题或前面一些问题,这就是递归问题,递归(recurrence)又称为递推.

可以用递归法定义集合.

(3) **递归法**　首先给出这个集合的初始元素;然后给出由集合中已知元素构造其他元素的方法;最后强调,有限次使用前面的步骤得到的元素是集合中仅有的元素.

【例 1-1】　自然数集合 $\mathbf{N}$ 可以递归定义如下:

首先,$0\in\mathbf{N}$;

其次,若 $n\in\mathbf{N}$,则 n 的后继 $n+1\in\mathbf{N}$;

最后,有限次使用前面的步骤得到的元素是集合 $\mathbf{N}$ 中仅有的元素.

集合的递归定义中,最后步骤很重要,它强调除有限次使用前面的步骤得到的元素是集合中元素外,不含有别的元素. 不过,请大家注意递归或递推和迭代的区别及联系[3].

在计算机科学中,还可以用别的方法定义集合,例如定义一种程序设计语言的语法时常采用的 BNF 范式法等(参见编译原理课程).

若集合 A 是有限集合,则用 $|A|$ 表示集合 A 中的元素个数,它与函数项级数收敛点的多少密切相关. 在中学使用的记号是 card(A).

需要注意的是,集合中的元素可以是任意对象,如元素本身又可以是集合等. 例如 $A=\{a,\{a,b\},b,c\}$,这时 $|A|=4$,即 A 中有 4 个元素,分别是 $a,\{a,b\},b,c$.

思考　所有不以自身为元素的集合能构成集合吗?

这是一个著名的罗素(B. A. M. Russell)悖论. 该集合悖论的出现引发了数学的第三次危机. 所谓悖论,就是逻辑上不一致. 假设存在这样的集合 $A=\{X\mid X\notin X\}$,则无论 $A\in A$ 或 $A\notin A$ 都是矛盾的. 避免这种悖论的方法是指定全集[4],这就是强调全集的重要性. 而信息科学中出现的集合不会有悖论,因此本书不讨论公理化集合论.

在没有特别说明的情况下,集合之间的元素是没有次序的,前面的集合 A 也可以记为 $A=\{a,b,c,\{a,b\}\}$等. 注意,程序是有序集合. 同时,若没有特别说明,所讨论的集合不是多重集,即集合中的元素原则上不重复,所以集合$\{a,\{a,b\},b,b,c\}$就是集合 A.

若集合 A 中有两个 a 元素,五个 b 元素,无限多个 c 元素,则 A 是可重集,这时 A 可以表示为 $A=\{2\cdot a,5\cdot b,\infty\cdot c\}$. 可重集在讨论组合计数时经常用到.

把不含有任何元素的集合称为**空集**(empty set),记为$\varnothing$或$\{\ \}$.

1.1.2　子集

一般来说,集合的子集比其本身要“小”一些.

【定义 1-1】　给定两个集合 A 和 B,若 A 中的任意元素都属于 B,则称 A 是 B 的**子集**(subset),或称 A 包含在 B,或称 B 包含 A,记为 $A\subseteq B$,如图 1-2 所示.

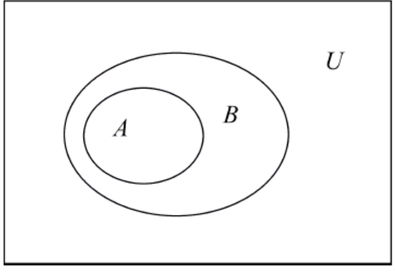


图　1-2

若 A 不是 B 的子集,这时集合 A 中至少有一个元素不属于 B.

显然有下面的定理.

【定理 1-1】　对于任意的集合 A,有$\varnothing\subseteq A$.

若两个集合 A,B 有完全相同的元素,则称这两个集合**相等**,记为 $A=B$.

我们有下述结论.

【定理 1-2】 设 A,B,C 是任意集合，下列结论成立.

(1) $A\subseteq A$；

(2) 若 $A\subseteq B$ 且 $B\subseteq A$，则 $A=B$；

(3) 若 $A\subseteq B$ 且 $B\subseteq C$，则 $A\subseteq C$.

我们知道，上述定理中结论(2)的逆也成立，这就是定理 1-3.

【定理 1-3】 $A=B$ 的充要条件是 $A\subseteq B$ 且 $B\subseteq A$.

该定理是证明两个集合相等的基本方法.

【定义 1-2】 若 $A\subseteq B$ 且 $A\neq B$，则称 A 是 B 的**真子集**(proper subset)，记为 $A\subset B$.

需要注意"$\in$"与"$\subseteq$"的区别，前者讨论的是元素与集合的关系，后者讨论的是集合与集合的关系，参见下面的例子.

【例 1-2】 设 A,B,C 是任意集合，若 $A\subseteq B, B\in C$，是否必有 $A\subseteq C$?

解 不成立. 例如，$A=\{a,b\}$，$B=\{a,b,c\}$，$C=\{a,\{a,b,c\}\}$，这时有 $A\subseteq B, B\in C$，而因为 $b\notin C$，所以结论不成立.

注意 在很多情况下，可以直接根据已知条件得出结论，但对于有些问题的讨论，举反例是一种最具说服力的方法.

1.1.3 幂集

【定义 1-3】 给定集合 X，由 X 的所有子集组成的集合称为 X 的**幂集**(power set)，记为 $P(X)$，即

$$P(X)=\{A \mid A\subseteq X\}$$

$P(X)$也可以记为 2^X，这种记法与下面的定理 1-4 有一定的关系.

【例 1-3】 设 $X=\{a,\{a,b\}\}$，计算 $P(X)$.

解 X 的子集有：空集$\varnothing$；由一个元素构成的子集$\{a\}$，$\{\{a, b\}\}$；由两个元素构成的子集$\{a,\{a, b\}\}$. 于是 $P(X)=\{\varnothing,\{a\},\{\{a, b\}\},\{a,\{a, b\}\}\}$.

【定理 1-4】 若$|X|=n$，则$|P(X)|=2^n$.

证 $\varnothing$是 X 的一个子集；由 X 中一个元素构成的子集有 C_n^1 个；由 X 中两个元素构成的子集有 C_n^2 个；…；由 X 中 $n-1$ 个元素构成的子集有 C_n^{n-1} 个；由 X 中 n 个元素构成的子集有 C_n^n 个. 因此，由加法原理和二项式定理知 X 的子集合共有

$$1+C_n^1+C_n^2+\cdots+C_n^{n-1}+C_n^n=(1+1)^n=2^n(\text{个})$$

上述定理也可以用乘法原理很方便证得，见习题 1.1.

1.1.4 *n* 元组

下面用最简洁方式介绍 n 元组.

【定义 1-4】 论域 U 中选取的 n 个元素 $x_1,x_2,\cdots,x_n$ 按照一定顺序排列，就得到一个 n 元有序组，简称 ***n* 元组**(ordered n-tuple)，记为$(x_1,x_2,\cdots,x_n)$或$\langle x_1,x_2,\cdots,x_n\rangle$.

在不强调排列的元素个数时，可以简称**元组**.

线性代数中的 n 维向量是 n 元组，有 n 个元素的字符串是 n 元组. n 元组$(x_1,x_2,\cdots,x_n)$中，x_i称为第 i 分量或第 i 位置元素$(1\leqslant i\leqslant n)$，它本身又可以是集合.

平面直角坐标系中任意一个点用 2 元组表示；空间直角坐标系中任意一个点用 3 元组

表示.

n 元组在数据结构中是一个线性表、栈或队列,在数据库中是一条记录,如(张三,男,19,重庆).

显然,两个 n 元组$(x_1,x_2,\cdots,x_n)$和$(y_1,y_2,\cdots,y_n)$相同的充要条件是其对应的分量或坐标相同,即 $x_i=y_i, 1\leqslant i\leqslant n$.

一般来说,$(x,y)\neq(y,x)$. 例如 2 元组$(2, 3)$和$(3, 2)$是不相同的,这一点可以在平面直角坐标系下直观地看出. 同时,$((a,b),c)$是 2 元组,它与 2 元组$(a,(b,c))$是不同的.

通常把 2 元组称为**有序对**或**序偶**(ordered pair).

1.1.5 笛卡儿积

给定一些集合,可以按下列方式构造出"新"的集合.

【定义 1-5】 设 $A_1,A_2,\cdots,A_n$ 是集合,称集合$\{(x_1,x_2,\cdots,x_n)\mid x_i\in A_i, i=1,2,\cdots,n\}$为 $A_1,A_2,\cdots,A_n$ 的**笛卡儿积**(Cartesian product)、**直积**(product set)或称为**叉积**(cross product),记为 $A_1\times A_2\times\cdots\times A_n$.

解析几何之父笛卡儿(R. Cartesian,1596—1650)是法国数学家,"我思故我在"和"越学习越发现自己无知"是他的名言.

由定义可知,笛卡儿积是一个集合,该集合中的元素是 n 元组. 为了方便,将 $\overbrace{A\times A\times\cdots\times A}^{n个}$ 记为 A^n.

【例 1-4】 设 $A=\{a,b\}, B=\{1,2\}, C=\{\varnothing\}$,试分别计算 $A\times B, B\times A, B\times C$ 和 $A\times B\times C$.

解 $A\times B=\{(a,1),(a,2),(b,1),(b,2)\}$, $B\times A=\{(1,a),(2,a),(1,b),(2,b)\}$,

$B\times C=\{(1,\varnothing), (2,\varnothing)\}$,

$A\times B\times C=\{(a, 1, \varnothing),(a, 2, \varnothing), (b, 1, \varnothing),(b, 2, \varnothing)\}$.

根据定义有 $A\times\varnothing=\varnothing\times A=\varnothing$,一般来说 $A\times B\neq B\times A$.

利用乘法原理,容易证明:

【定理 1-5】 若$|A|=m$, $|B|=n$,则$|A\times B|=mn$.

习 题 1.1

1. 用列举法表示下列集合:

(1) $\{x\mid x\in\mathbf{R}, x^2-5x+6=0\}$;

(2) $\{2x\mid x\in\mathbf{N}\}$.

2. 写出 35 的所有因数集合及 D_{35}.

3. 比较集合$\varnothing$,$\{\varnothing\}$和$\{\{\varnothing\}\}$的不同之处.

4. 判定下列断言是否成立,说明理由:

(1) $\varnothing\subseteq\varnothing$;

(2) $\varnothing\in\varnothing$;

(3) $\varnothing\subseteq\{\varnothing\}$;

(4) $\varnothing\in\{\varnothing\}$.

5. 设 A 和 B 是集合,试举出使 $A\in B$ 且 $A\subseteq B$ 同时成立的例子.

6. 对于任意集合 A,B,C,判定下列断言是否成立,说明理由:

(1) 若 $A\subseteq B$ 且 $B\in C$,则 $A\notin C$;

(2) 若 $A\subseteq B$ 且 $B\in C$,则 $A\subseteq C$;

(3) 若 $A\in B$ 且 $B\in C$,则 $A\in C$;

(4) 若 $A\in B$ 且 $B\in C$,则 $A\subseteq C$.

7. 分别计算:

(1) $P(P(\varnothing))$;

(2) $P(\{a, b, c\})$;

(3) $P(\{\{a,b,c\}\})$.

8. 试用乘法原理证明定理 1-4.

9. 证明定理 1-5.

10. 设 $A=\{a,b\}$,$B=\{1,2,3\}$,试分别计算:

$$A\times A, A\times B, B\times A, A\times B\times A, (A\times B)\times A$$

11. 对于任意集合 A,B,C,由 $A\times B=A\times C$ 能否得出 $B=C$,为什么?若 $A\neq\varnothing$ 呢?

12. 设 $|S|=n$,给出一种列出 S 的所有子集的方法.

1.2 映射的有关概念

1.2.1 映射的定义

映射就是函数.函数是在 17 世纪 30 年代研究曲线运动时产生的一个概念,虽然这个概念在 1673 年才由 G. W. Leibniz(1646—1716)开始使用,而函数表达式 $f(x)$ 在 1734 年才由 L. Euler(1707—1783)引入.

当今函数研究的是任意两个集合之间的一种对应关系,它将其中一个集合的元素按某种规则指定为另一个集合中的元素.在中学及高等数学中讨论的函数是在实数范围内进行的.

映射也是现代数学中的基本概念,要求我们在各学科中都要会使用映射的观点.函数在信息科学中得到了充分的应用,编写 C 语言程序就是编写函数,实际上计算机的任何输出都可以看作是某些输入的函数.同时,借助于映射思想,可以得出一些较深入的结论.

与集合一样,映射贯穿本书的所有内容.深刻理解映射有关内容,对于其他内容的学习是至关重要的.当然,这部分内容本身是重点,也是难点.

【定义 1-6】 任意给定两个集合 A 和 B,若存在对应法则 f,使得对于任意 $x\in A$,均存在唯一的 $y\in B$ 与它对应,则称 f 是集合 A 到 B 的一个**映射**(mapping),或称其为 A 到 B 的一个**函数**(function),记为 $f:A\rightarrow B$(如图 1-3 所示).

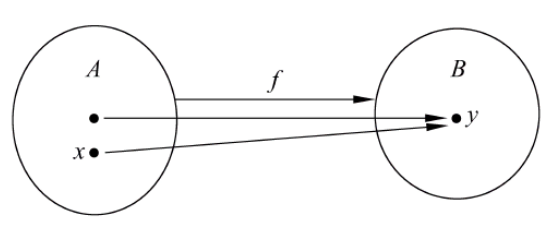


图 1-3

在实际应用中通常将 A 到 A 的映射称为 A 上的变换(transformation).

有些映射可以采用解析表达式表示，如 f：$\mathbf{R}\to\mathbf{R}$，$y=f(x)=x^2+1$.

函数 g：$\mathbf{Z}\to\mathbf{N}$，其中

$$y=g(x)=\begin{cases}1, & x\text{ 为奇数}\\ 0, & x\text{ 为偶数}\end{cases}$$

是分段函数.

假定 A 是论域 U 上的集合，可以定义为 $\mu_A:U\to[0,1]$，其中

$$\mu_A(x)=\begin{cases}1, & x\in A\\ 0, & x\notin A\end{cases},$$

这里 μ_A 称为集合 A 的特征函数.

下面介绍两个计算机科学中广泛应用的实数集 $\mathbf{R}$ 到整数集 $\mathbf{Z}$ 的函数：$\lceil x\rceil$ 和 $\lfloor x\rfloor$. 对于任意实数 x，用 $\lceil x\rceil$ 表示大于等于 x 的最小整数，称为**天花板函数**(ceiling function). 用 $\lfloor x\rfloor$ 表示小于等于 x 的最大整数，称为**地板函数**(floor function). 通常，**取整函数**$[x]$是地板函数. 例如，$\lceil 1.4\rceil=2$，$\lceil -1.4\rceil=-1$，$\lfloor 1.4\rfloor=1$，$\lfloor -1.4\rfloor=-2$. 显然，有 $x-1<\lfloor x\rfloor\leqslant x\leqslant\lceil x\rceil<x+1$. 最接近实数 x 的整数为 $\lceil x-0.5\rceil$ 或 $\lfloor x+0.5\rfloor$，除非 x 位于两个相邻整数的中间.

在算法分析时，复杂度均为正整数集合 $\mathbf{Z}^+$ 到正实数集合 $\mathbf{R}^+$ 的函数，例如利用冒泡算法对 n 个实数按从小到大顺序排序的执行时间为 $T(n)=\frac{a}{2}n(n-1)+b$，其中 a 和 b 为常数[20].

函数符号通常用一个英文字母 $f,g,h,F,G,H,\cdots$ 或希腊字母 $\varphi,\psi,\cdots$ 表示(可以带下标)，也可以根据具体情况选用几个字母表示，如 sin，cos，tan，exp，max，min，add，root，average，hanoi，delete_string，…

假定 $f:A\to B$，$y=f(x)$，通常把 x 称为自变量，自变量的取值范围称为**定义域**(domain)，记为 dom$f$. 将 y 称为因变量，而把函数值所在范围称为**值域**(range)，记为 ran$f$.

这里讨论的映射有两个特点：

(1) 函数 f 的定义域是集合 A，因而这里定义的函数是全函数，而不是一般意义下的偏函数，即 dom $f\subseteq A$；

(2) 任意 $x\in A$，对应于 B 中唯一的元素 $f(x)$，$f(x)$称为 x 在映射 f 下的函数值(但不一定是数)或称为 x 在映射 f 下的像，通常记为 $y=f(x)$.

对于集合 A 和 B，用 B^A(读作"B 上 A")表示 A 到 B 的所有映射组成的集合，即

$$B^A=\{f\mid f:A\to B\}$$

【例 1-5】 若 $A=\{x_1,x_2,x_3\}$，$B=\{y_1,y_2\}$，求 B^A.

解 A 到 B 的映射为 f_i，$i=1,2,\cdots,8$，其中：

$f_1(x_1)=y_1$，$f_1(x_2)=y_1$，$f_1(x_3)=y_1$；$f_2(x_1)=y_1$，$f_2(x_2)=y_1$，$f_2(x_3)=y_2$；
$f_3(x_1)=y_1$，$f_3(x_2)=y_2$，$f_3(x_3)=y_1$；$f_4(x_1)=y_1$，$f_4(x_2)=y_2$，$f_4(x_3)=y_2$；
$f_5(x_1)=y_2$，$f_5(x_2)=y_1$，$f_5(x_3)=y_1$；$f_6(x_1)=y_2$，$f_6(x_2)=y_1$，$f_6(x_3)=y_2$；
$f_7(x_1)=y_2$，$f_7(x_2)=y_2$，$f_7(x_3)=y_1$；$f_8(x_1)=y_2$，$f_8(x_2)=y_2$，$f_8(x_3)=y_2$.

【定理 1-6】 对于集合 A 和 B，若 $|A|=m$，$|B|=n$，则 $|B^A|=n^m$.

证 设 $f:A\to B$，对于任意的 $x\in A$，显然 $f(x)$可取 B 中 n 个元素中任意一个，而

$|A|=m$,根据乘法原理,结论成立.

【定义 1-7】 设 $f:A\to B$,令 $X\subseteq A$,用 $f(X)=\{f(x)\mid x\in X\}$表示 X 在映射 f 下的**像**(image).令 $Y\subseteq B$,用 $f^{-1}(Y)=\{x\mid f(x)\in Y\}$表示 Y 在映射 f 下的**原像**(inverse image).

注意 这里的 $f^{-1}(Y)$是一个整体记号.

在函数的定义中,假定 $A=A_1\times A_2\times\cdots\times A_n$,则任意 $x\in A$,有 $x=(x_1,x_2,\cdots,x_n)$,其中 $x_i\in A_i$,$1\leqslant i\leqslant n$.这时,

$$f(x)=f((x_1,x_2,\cdots,x_n))=:f(x_1,x_2,\cdots,x_n),$$

称 f 为 $A_1,A_2,\cdots,A_n$ 到 B 的 ***n* 元函数**(n-ary function).

显然,在 n 元函数 $f(x_1,x_2,\cdots,x_n)$中,参数位置是有次序的,当 $n=0$ 时,f 是 C 语言中的无参函数,可将 f 理解为 B 中的一个元素.如果 $f:\overbrace{A\times A\times\cdots\times A}^{n个}\to B$,则称 f 为 A 到 B 的 n 元函数.

函数可以递归定义,参见参考文献[5]及习题 1.2 的第 14 题.

图 1-4

思考 函数在计算机中是如何实现的(参见图 1-4)?

1.2.2 映射的性质

1. 单射

【定义 1-8】 假设 $f:A\to B$,如果对任意 $x_1,x_2\in A$,由 $f(x_1)=f(x_2)$可推出 $x_1=x_2$,则称 f 是 A 到 B 的**单射**(injection),或称 f 是 A 到 B 的一对一(one-to-one)映射.

等价地,对任意 $x_1,x_2\in A$,若 $x_1\neq x_2$,可得出 $f(x_1)\neq f(x_2)$,则称 f 是 A 到 B 的单射,如图 1-5(a)所示.

【例 1-6】 设 $f:\mathbf{N}\to\mathbf{N}$,$f(x)=2x$,则 f 是 $\mathbf{N}$ 到 $\mathbf{N}$ 的单射,试证明之.

证 对任意 $x_1,x_2\in\mathbf{N}$,由 $f(x_1)=f(x_2)$可得出 $2x_1=2x_2$,进而 $x_1=x_2$.

2. 满射

【定义 1-9】 假设 $f:A\to B$,如果对任意 $y\in B$,均存在 $x\in A$,使得 $y=f(x)$,则称 f 是 A 到 B 的**满射**(surjection),或称 f 是 A 到 B 的映上(onto)的映射.

显然,f 是 A 到 B 的满射的充要条件是 f 的值域为 B,即 $\mathrm{ran}f=B$,如图 1-5(b)所示.

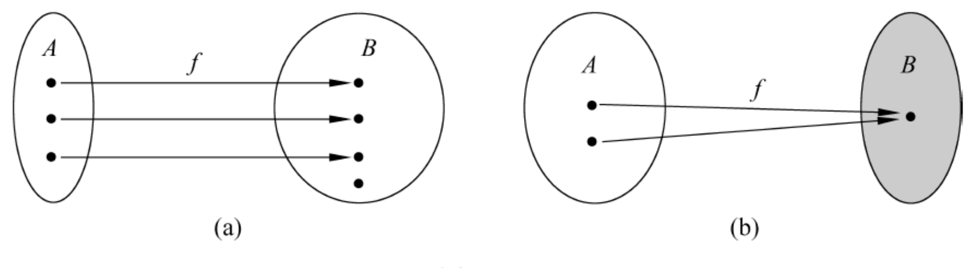


图 1-5

【例 1-7】 设 $f:\mathbf{Z}\to\mathbf{N}$,$f(x)=|x|$,则 f 是 $\mathbf{Z}$ 到 $\mathbf{N}$ 的满射,试证明之.

证 任意 $y\in\mathbf{N}$,取 $x=y\in\mathbf{Z}$,显然有 $y=f(x)$.

3. 双射

【定义 1-10】 假设 $f:A \to B$,若 f 既是单射又是满射,则称 f 是 A 到 B 的**双射**(bijection),或称 f 是 A 到 B 的**一一对应**(one-to-one correspondence).

【例 1-8】 试建立一个 $\mathbf{Z}$ 到 $\mathbf{N}$ 的一一对应.

解 令 $f:\mathbf{Z} \to \mathbf{N}$,

$$f(x)=\begin{cases}2x, & x \geqslant 0 \\ 2|x|-1, & x<0\end{cases}$$

很容易验证,f 是一个 $\mathbf{Z}$ 到 $\mathbf{N}$ 的一一对应.

事实上,$\mathbf{Z}$ 到 $\mathbf{N}$ 的一一对应不是唯一的. 记住:一一对应思想就是配对思想.

【例 1-9】 试建立一个(0,1)到 $\mathbf{R}$ 的一一对应.

解 令 $f:(0,1) \to \mathbf{R}, f(x)=\tan (x-1/2)\pi$.

【定义 1-11】 若A 是有限集合,通常把 A 到 A 的双射称为 A 上的**置换**(permutation).

【例 1-10】 写出 $A=\{1,2,3\}$上的所有置换.

解 $A=\{1,2,3\}$上的所有置换有 6 个,分别是:

$p_1(1)=1$, $p_1(2)=2$, $p_1(3)=3$; $p_2(1)=2$, $p_2(2)=1$, $p_2(3)=3$;

$p_3(1)=3$, $p_3(2)=2$, $p_3(3)=1$; $p_4(1)=1$, $p_4(2)=3$, $p_4(3)=2$;

$p_5(1)=2$, $p_5(2)=3$, $p_5(3)=1$; $p_6(1)=3$, $p_6(2)=1$, $p_6(3)=2$.

上面的 6 个置换常用另外两种方式书写,请自己总结书写方法.

第一种方式 $p_1=\begin{pmatrix}1 & 2 & 3\\1 & 2 & 3\end{pmatrix}$, $p_2=\begin{pmatrix}1 & 2 & 3\\2 & 1 & 3\end{pmatrix}$, $p_3=\begin{pmatrix}1 & 2 & 3\\3 & 2 & 1\end{pmatrix}$,

$p_4=\begin{pmatrix}1 & 2 & 3\\1 & 3 & 2\end{pmatrix}$, $p_5=\begin{pmatrix}1 & 2 & 3\\2 & 3 & 1\end{pmatrix}$, $p_6=\begin{pmatrix}1 & 2 & 3\\3 & 1 & 2\end{pmatrix}$.

第二种方式 $p_1=(1)(2)(3)$, $p_2=(12)(3)$, $p_3=(13)(2)$,

$p_4=(1)(23)$, $p_5=(123)$, $p_6=(132)$.

利用置换可以对信息加密,例如给定 26 个英文字母的一个置换:

$$p=\begin{pmatrix}\mathrm{a} & \mathrm{b} & \mathrm{c} & \mathrm{d} & \mathrm{e} & \mathrm{f} & \mathrm{g} & \mathrm{h} & \mathrm{i} & \mathrm{j} & \mathrm{k} & \mathrm{l} & \mathrm{m} & \mathrm{n} & \mathrm{o} & \mathrm{p} & \mathrm{q} & \mathrm{r} & \mathrm{s} & \mathrm{t} & \mathrm{u} & \mathrm{v} & \mathrm{w} & \mathrm{x} & \mathrm{y} & \mathrm{z}\\ \mathrm{f} & \mathrm{j} & \mathrm{h} & \mathrm{l} & \mathrm{d} & \mathrm{n} & \mathrm{q} & \mathrm{k} & \mathrm{x} & \mathrm{p} & \mathrm{s} & \mathrm{a} & \mathrm{v} & \mathrm{y} & \mathrm{b} & \mathrm{o} & \mathrm{g} & \mathrm{w} & \mathrm{t} & \mathrm{m} & \mathrm{r} & \mathrm{c} & \mathrm{i} & \mathrm{u} & \mathrm{z} & \mathrm{e}\end{pmatrix},$$

可将 i love you 写成 x abcd zbr,其中 i love you 是**明文**(plaintext),x abcd zbr 是**密文**(ciphertext),p 是**密钥**(key).

1.2.3 逆映射

设 $f:A \to B$ 如图 1-6(a)所示,将 f 的方向逆转后如图 1-6(b)所示的 f^{-1},易见 f^{-1}不是 B 到 A 的映射.

【定义 1-12】 设 $f:A \to B$,如果将对应关系 f 的方向逆转后,可得到一个集合 B 到集合 A 的映射,则该映射称为 f 的**逆映射**或**逆函数**(常称为**反函数**,invertible function),记为 f^{-1}.

假定 $f:A \to B$,将对应关系 f 的方向逆转后能得到 B 到 A 的映射,第一,f 必须是单射;第二,f 必须是满射. 于是有下述定理.

【定理 1-7】 设 $f:A \to B$,则 f 的逆映射存在的充要条件是 f 是双射.

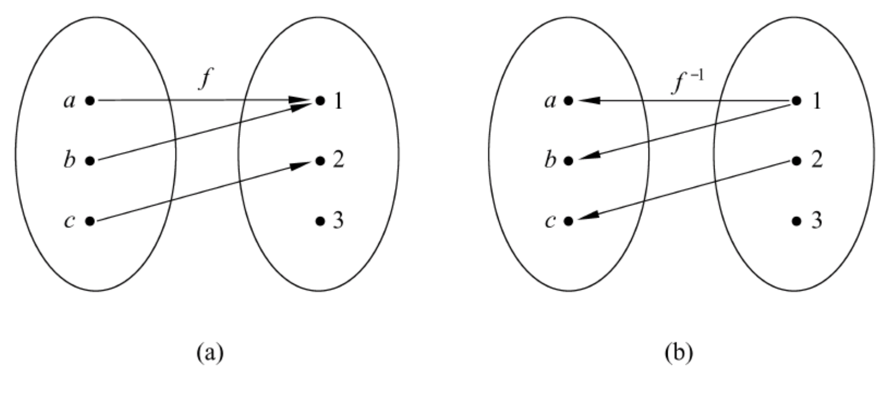


图 1-6

回忆一下，在以前学习反函数时为何有一些限制条件，如正弦函数 $y=\sin x$，为了讨论其反函数，通常限制 $x\in[-\pi/2,\pi/2]$，就是为了保证 $\sin:[-\pi/2,\pi/2]\to[-1,1]$是一个双射(一一对应).

显然，双射 $f:A\to B$ 的逆映射 $f^{-1}:B\to A$ 也是双射且$(f^{-1})^{-1}=f$.

【例 1-11】 判定所给出的映射是否有逆映射，若有，请求出其逆映射.

(1) $f:\mathbf{R}\to\mathbf{R}, f(x)=x^2$；

(2) $g:\mathbf{R}\to\mathbf{R}, g(x)=x^3$.

解 (1) 因为 $f(2)=f(-2)=4$，f 不是单射，所以 f 不存在逆映射.

(2) 显然，g 是双射，其逆映射为 $g^{-1}:\mathbf{R}\to\mathbf{R}, g^{-1}(y)=\sqrt[3]{y}$(如 $g(-3)=-27$，于是有 $g^{-1}(-27)=-3$).

1.2.4 复合映射

显然，我们有

【定理 1-8】 设$f:A\to B, g:B\to C$，对于任意 $x\in A$，令 $h(x)=g(f(x))$，则 h 是集合 A 到集合 C 的映射.

于是有定义

【定义 1-13】 设 $f:A\to B, g:B\to C$，对任意 $x\in A, h(x)=g(f(x))$，则称 h 为 f 和 g 的**复合映射或复合函数**(composition of f and g)，记为 $f\circ g$.

映射 f 和 g 的复合映射 $f\circ g$ 可以按图 1-7 方式理解.

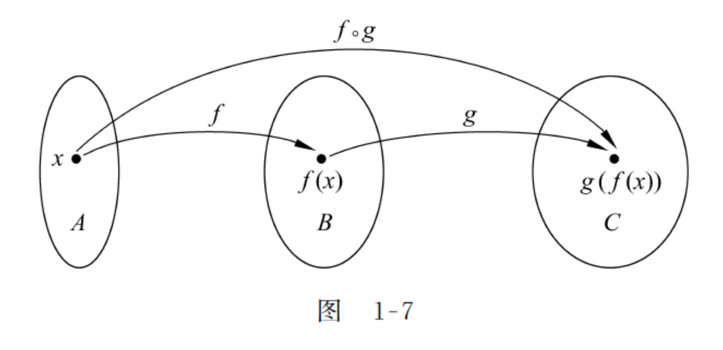


图 1-7

由复合函数的定义知，

$$(f\circ g)(x)=g(f(x))$$

注意到 f 和 g 的复合是记为 $f\circ g$，要求从左至右进行. 它与传统的两个函数复合的记号在次序上不尽一致，显得也不太自然，若将函数 f 对 x 的作用的方式写成 x^f 形式，则

$$x^{f\circ g} = (x^f)^g$$

就比较自然了.

之所以这样处理，是考虑到今后要定义的两个对象参加运算都是从左至右进行的(当然包括以前学过的运算).

【例 1-12】 设 $A=\{a,b,c\}$，$B=\{1,2,3\}$，$C=\{\alpha,\beta,\gamma,\delta\}$，令 $f:A\to B$，$g:B\to C$，$f(a)=2$，$f(b)=3$，$f(c)=3$，$g(1)=\beta$，$g(2)=\alpha$，$g(3)=\delta$. 试计算复合映射 $f\circ g$.

解 复合映射 $f\circ g:A\to C$，$(f\circ g)(a)=g(f(a))=g(2)=\alpha$，$(f\circ g)(b)=g(f(b))=g(3)=\delta$，$(f\circ g)(c)=g(f(c))=g(3)=\delta$.

注意 复合映射又称为复合函数. 要保证复合映射 $f\circ g$ 有意义，必须

$$f(A)\subseteq \mathrm{dom}(g)$$

【例 1-13】 设 $\mathbf{R}$ 到 $\mathbf{R}$ 有两个映射 f 和 g，定义如下：$f(x)=x^2$，$g(x)=x+2$，试分别计算复合映射 $f\circ g$ 和 $g\circ f$.

解 对任意 $x\in\mathbf{R}$，分别有

$$(f\circ g)(x) = g(f(x)) = g(x^2) = x^2+2$$
$$(g\circ f)(x) = f(g(x)) = f(x+2) = (x+2)^2$$

对于例 1-13 来说，计算两个函数的复合可以采用高等数学中的方法，要求计算 $g(f(x))$ 以及 $f(g(x))$ 更明确些.

注意 一般说来，即使复合映射 $f\circ g$ 和 $g\circ f$ 均有意义，也不能保证 $f\circ g=g\circ f$ 成立.

设 A 是集合，令 $f:A\to A$，$f(x)=x$，称 f 为集合 A 上的**恒等映射**(identity function on A)，记为 I_A.

显然有下述结论：

【定理 1-9】 若 $f:A\to B$ 是双射，则有 $f\circ f^{-1}=I_A$，$f^{-1}\circ f=I_B$. 特别地，若 $f:A\to A$ 是双射，则 $f\circ f^{-1}=f^{-1}\circ f=I_A$.

下面的定理讨论了映射的性质与复合映射之间的关系.

【定理 1-10】 设 $f:A\to B$，$g:B\to C$.

(1) 若 f 和 g 是单射，则 $f\circ g$ 是单射；

(2) 若 f 和 g 是满射，则 $f\circ g$ 是满射；

(3) 若 f 和 g 是双射，则 $f\circ g$ 是双射且 $(f\circ g)^{-1}=g^{-1}\circ f^{-1}$.

证 (1) 对任意 $x_1,x_2\in A$，假定 $(f\circ g)(x_1)=(f\circ g)(x_2)$，即 $g(f(x_1))=g(f(x_2))$. 已知 g 是单射，于是有 $f(x_1)=f(x_2)$. 由于 f 是单射，所以 $x_1=x_2$. 进而 $f\circ g$ 是单射.

(2)和(3)作为练习.

【定理 1-11】 设 $f:A\to B$，$g:B\to C$，

(1) 若 $f\circ g$ 是单射，则 f 是单射，但 g 不一定；

(2) 若 $f\circ g$ 是满射，则 g 是满射，而 f 不一定.

证 (1) 作为练习.

(2) 对于任意 $z\in C$，由于 $f\circ g$ 是满射，必存在 $x\in A$，使得 $(f\circ g)(x)=g(f(x))=z$. 令 $y=f(x)\in B$，有 $g(y)=z$，因此，g 是满射.

设 $A=\{a,b,c\}$，$B=\{1,2,3\}$，$C=\{\alpha,\beta\}$，令 $f:A\to B$，$g:B\to C$，$f(a)=2$，$f(b)=3$，$f(c)=3$，$g(1)=\beta$，$g(2)=\alpha$，$g(3)=\beta$. 这时，$(f\circ g)(a)=g(f(a))=\alpha$，$(f\circ g)(b)=g(f(b))=\beta$，显然有 $\text{ran}(f\circ g)=\{\alpha,\beta\}$，$f\circ g$ 是满射. 而 $\text{ran}\ f=\{2,3\}$，f 不是满射.

下面的定理会经常使用.

【定理 1-12】 设 $f:A\to B$，$g:B\to C$，$h:C\to D$，则 $(f\circ g)\circ h=f\circ(g\circ h)$.

证 对任意 $x\in A$，由于 $((f\circ g)\circ h)(x)=h[(f\circ g)(x)]=h[g(f(x))]$，而 $(f\circ(g\circ h))(x)=(g\circ h)(f(x))=h[g(f(x))]$，由此可见，$((f\circ g)\circ h)(x)=(f\circ(g\circ h))(x)$. 所以 $(f\circ g)\circ h=f\circ(g\circ h)$.

注意 由定理 1-12 可知，多个函数求复合时可以不加括号，即 $f\circ g\circ h=(f\circ g)\circ h=f\circ(g\circ h)$.

习 题 1.2

1. 分别计算 $\lceil 1.5\rceil$，$\lceil -1\rceil$，$\lceil -1.5\rceil$，$\lfloor 1.5\rfloor$，$\lfloor -1\rfloor$，$\lfloor -1.5\rfloor$.

2. 下列映射中，哪些是双射？说明理由.

(1) $f:\mathbf{Z}\to\mathbf{Z}$，$f(x)=3x$；

(2) $f:\mathbf{Z}\to\mathbf{N}$，$f(x)=|x|+1$；

(3) $f:\mathbf{R}\to\mathbf{R}$，$f(x)=x^3+1$；

(4) $f:\mathbf{N}\times\mathbf{N}\to\mathbf{N}$，$f(x_1,x_2)=x_1+x_2+1$；

(5) $f:\mathbf{N}\to\mathbf{N}\times\mathbf{N}$，$f(x)=(x,x+1)$.

3. 对于有限集合 A 和 B，假定 $f:A\to B$ 且 $|A|=|B|$，证明：f 是单射的充要条件是 f 是满射. 对于无限集合，上述结论成立吗？举例说明.

4. 设 $f:A\to B$，试证明：

(1) $f\circ I_B=f$；

(2) $I_A\circ f=f$.

特别地，若 $f:A\to A$，则 $f\circ I_A=I_A\circ f=f$.

5. 试举出一个例子说明 $f\circ f=f$ 成立，其中 $f:A\to A$ 且 $f\neq I_A$. 若 f 的逆映射存在，满足条件的 f 还存在吗？

6. 设 $f:A\to B$，$g:B\to C$. 若 f 和 g 是满射，则 $f\circ g$ 是满射，试证明.

7. 设 $f:A\to B$，$g:B\to C$. 试证明：若 $f\circ g$ 是单射，则 f 是单射. 试举例说明，这时 g 不一定是单射.

8. 设 $f:A\to B$，若存在 $g:B\to A$，使得 $f\circ g=I_A$ 且 $g\circ f=I_B$，试证明：f 是双射且 $f^{-1}=g$.

9. 设 $f:A\to B$，$g:B\to C$. 若 f 和 g 是双射，则 $f\circ g$ 是双射且 $(f\circ g)^{-1}=g^{-1}\circ f^{-1}$.

10. 设 G 是集合 A 到 A 的所有双射组成的集合，证明：

(1) 任意 $f,g\in G$，有 $f\circ g\in G$；

(2) 对于任意 $f,g,h\in G$，有 $(f\circ g)\circ h=f\circ(g\circ h)$；

(3) $I_A\in G$ 且对于任意 $f\in G$，有 $I_A\circ f=f\circ I_A=f$；

(4) 对于任意 $f\in G$,有 $f^{-1}\in G$ 且 $f\circ f^{-1}=f^{-1}\circ f=I_A$.

11. 若 $A=\{a, b, c\}$,$B=\{1, 2\}$,问 A 到 B 的满射、单射、双射各有多少个?试推广你的结论.

12. 设 A, B, C, D 是任意集合,f 是 A 到 B 的双射,g 是 C 到 D 的双射,令 $h:A\times C\to B\times D$,对任意$(a,c)\in A\times C$,$h(a,c)=(f(a),g(c))$. 证明:h 是双射.

13. 设 $f:A\to B$,$g:B\to C$,$h:C\to A$. 证明:若 $f\circ g\circ h=I_A$,$g\circ h\circ f=I_B$,$h\circ f\circ g=I_C$,则 f,g,h 均可逆. 求出 f^{-1},g^{-1},h^{-1}.

14. 已知阿克曼(Ackermann)函数 $A:\mathbf{N}\times\mathbf{N}\to\mathbf{N}$ 的定义为:

(1) $A(0,n)=n+1$,$n\geqslant 0$;

(2) $A(m,0)=A(m-1,1)$,$m>0$;

(3) $A(m,n)=A(m-1,A(m,n-1))$,$m>0$,$n>0$.

分别计算 $A(2,3)$和 $A(3,2)$.

1.3 运算的定义及性质

运算是由已知对象得出新对象的一种方法. 其实,已经接触过很多运算,如数之间的加法运算、多项式之间的乘法运算、矩阵的逆运算、向量的线性运算等. 在讨论离散数据结构时也会经常遇到各种各样的运算,如在 1.4 节即将研究的集合间的运算.

虽然运算本质上是映射,但研究的侧重点不同,在运算中更注重于运算满足的一些运算性质,而根据这些性质可以对一些离散对象分门别类进行讨论,参见代数结构章节.

运算器是计算机的四大零部件之一。本节将对运算的一般定义及其性质进行抽象讨论.

1.3.1 运算的定义

【定义 1-14】 设 A_1,A_2,…,A_n 和 B 是集合,若

$$f:A_1\times A_2\times\cdots\times A_n\to B$$

则称 f 为 A_1,A_2,…,A_n 到 B 的 n **元运算**(operation).

在不需要强调集合 A_1,A_2,…,A_n 和 B 时,可简称 f 为**运算**. 若 $f:\overbrace{A\times A\times\cdots\times A}^{n个}\to B$,则称 f 为 A 到 B 的 n 元运算,或称为 A 上的 n 元运算.

若对于任意 x_1,x_2,…,$x_n\in A$,有 $f(x_1,x_2,\cdots,x_n)=y\in A$,则称 f 为 A 上的 n 元**封闭运算**(closed operation),或称为 A 上的 n 元**代数运算**.

设 f 为 A_1,A_2,…,A_n 到 B 的 n 元运算,在 $y=f(x_1,x_2,\cdots,x_n)$中,x_1,x_2,…,x_n 是参加运算的 n 个有顺序的对象,正因为这样 f 称为 n 元运算,y 是运算结果,由定义知道,运算结果一定是唯一的.

【例 1-14】 设 $f:\mathbf{Z}\to\mathbf{N}$,$f(x)=|x|$,这时,$f$ 是整数集合 $\mathbf{Z}$ 上的取绝对值运算,f 是 1 元运算.

下面介绍数论中的一些非常重要的运算.

对于任意整数 m 和 n,当 $m\neq 0$ 时,必存在唯一整数 q 和 r,使得 $n=qm+r(0\leqslant r<|m|)$,这就是带余除法,其中 q 称为**商**(quotient),r 称为**余数**(remainder),可由长除法求

得. 注意余数 $0 \leqslant r < |m|$,而在 C 语言中 $n\%m$ 得到一个与 n 符号一致的余数 r,$0 \leqslant |r| < m$.

利用带余除法,可以将十进制数与其他进制的数进行转换. 例如十进制数 247 转换成八进制可以这样做:$247 = 30 \times 8 + 7$,$30 = 3 \times 8 + 6$,于是

$$247 = 30 \times 8 + 7 = (3 \times 8 + 6) \times 8 + 7 = 3 \times 8^2 + 6 \times 8 + 7,$$

因此,$247 = (367)_8$.

【例 1-15】(模运算) 对于固定的正整数 m,设 $f: \mathbf{Z} \to \mathbf{N}$,$f(x) = x(\bmod m)$,$x(\bmod m)$ 是整数 x 除以 m 的余数. 根据带余除法知,$x(\bmod m)$是使 $x = qm + r$,$0 \leqslant r < m$ 成立的整数 r. 这里,f 是 $\mathbf{Z}$ 上的模 m 运算,是 1 元运算.

容易证明:对于正整数 m 和任意整数 x 和 y,有

$$(x + y)(\bmod m) = (x(\bmod m) + y(\bmod m))(\bmod m),$$

$$(x \cdot y)(\bmod m) = (x(\bmod m) \cdot y(\bmod m))(\bmod m).$$

模运算的两个最简单的应用.

将 26 个英文字母 $a, b, c, \cdots, z$ 分别对应于整数 $0, 1, 2, \cdots, 25$,为了保密,可以将每一个字母往后推移 3 位,若接收到的密文为 l oryh brx,则明文为 i love you. 这时的加密变换为 $c = (p + 3)(\bmod 26)$,解密变换为 $p = (c - 3)(\bmod 26)$,其中 p 是明文对应的整数,c 是密文对应的整数,3 是密钥. 这种密码称为凯撒(J. Caesar)密码,早在公元前罗马皇帝凯撒就使用该方法传递作战命令.

将大量记录存放在 m 个不同的链表,可以将每个记录的识别码 n 进行模 m 运算,运算结果为该记录所在的链表,即 $h(n) = n(\bmod m)$. 通常将 h 称为**散列函数**或**哈希函数**(Hash function).

【例 1-16】 设 $f: \mathbf{Q} \times \mathbf{Q} \to \mathbf{R}$,$f(x_1, x_2) = x_1 + \sqrt[3]{x_2}$,这时,$f$ 是 $\mathbf{Q}$ 上的加法运算,f 是 2 元运算. 又设 $f: \mathbf{R} \times \mathbf{R} \times \mathbf{R} \to \mathbf{R}$,$f(x_1, x_2, x_3) = x_1^2 + x_2 x_3$,这时,$f$ 是 $\mathbf{R}$ 上的 3 元封闭运算.

【例 1-17】 对于给定的正整数 m,整数集合 $\mathbf{Z}$ 上模 m 加法运算"$+_m$"和模 m 乘法运算"$\cdot_m$"分别定义如下:对于任意整数 x 和 y,$x +_m y = (x + y)(\bmod m)$,$x \cdot_m y = (xy)(\bmod m)$. 例如 $m = 5$,$3 +_3 (-5) = (-2)(\bmod 3) = 1$,$3 \cdot_3 (-5) = (-15)(\bmod 3) = 0$.

实际上,模 m 加法运算"$+_m$"和模 m 乘法运算"$\cdot_m$"是 $\mathbf{Z}_m = \{0, 1, 2, \cdots, m-1\}$上的封闭运算,见习题 1.3 第 12 题.

【例 1-18】 整数集合 $\mathbf{Z}$ 上两个二元运算 gcd 和 lcm.

(1) 对于任意整数 m, n,若 $d|m$ 且 $d|n$,则称 d 为 m 和 n 的**公因数**(common divisor). 例如,由于 $-2|4$ 且 $-2|-6$,所以 -2 是 4 和 -6 的公因数. 容易知道,4 和 -6 的所有公因数为 $-1, -2, 1$ 和 2,其最大公因数为 2. 用 $\gcd(m, n)$表示 m 和 n 的**最大公因数**(greatest common divisor)(必为正整数),但 gcd 不是整数集合 $\mathbf{Z}$ 上的二元运算,因为任何整数都是 0 的因数,于是 $\gcd(0, 0)$不存在. 若集合 $A = \{1,2,3,4,5,6\}$,这时 gcd 是 A 上的封闭 2 元运算.

(2) 对于任意整数 m, n,若 $m|d$ 且 $n|d$,则称 d 为 m 和 n 的公倍数(common multiple).

例如,由于 $4|-12$ 且 $-6|-12$,所以 -12 是 4 和 -6 的公倍数. 4 和 -6 的公倍数很多,如 $-12,-24,12,24,36$ 等,其最小非负公倍数为 12. 用 $\mathrm{lcm}(m,n)$ 表示 m 和 n 的最小非负公倍数,简称**最小公倍数**(least common multiple),则 lcm 是整数集合 $\mathbf{Z}$ 上的封闭的二元运算. 显然,对于任意整数 $n\geqslant 0$,有 $\mathrm{lcm}(0, n)=0$,特别地,$\mathrm{lcm}(0, 0)=0$. 若集合 $A=\{1,2,3,4,5,6\}$,这时 lcm 不是 A 上的封闭 2 元运算,因为 $\mathrm{lcm}(4, -6)=12\notin A$.

运算符号 gcd 和 lcm 也可分别记为[,]和(,),即 $\gcd(m,n)=[m,n]$, $\mathrm{lcm}(m,n)=(m,n)$. 由于 $\gcd(m, n)=\gcd(|m|, |n|)$且 $\mathrm{lcm}(m, n)=\mathrm{lcm}(|m|, |n|)$,因此在很多的时候,我们讨论的是两个正整数的最大公因数和最小公倍数.

在理论上容易证明,对于大于 1 的正整数 n 都可以分解成一些素数乘积

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k},$$

其中 $p_1,p_2,\cdots,p_k$是不同的素数,$r_1,r_2,\cdots,r_k$是正整数,并且在不计素数顺序(或按从小到大顺序)的情况下,该分解方式是唯一的.

例如 $6=2\times 3$,$12=2^2\times 3$,$21560=2^3\times 5\times 7^2\times 11$,$1024=2^{10}$,但实际上对于较大的 n,要得出 n 的素因数分解,甚至找到 n 的一个素因数都是相当困难的. 到现在为止,还未找到当 $n=142022$ 时费马数 $F_n=2^{2^n}+1$ 的一个素因数.

若 $m=p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}\in\mathbf{Z}^+$,$n=p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}\in\mathbf{Z}^+$($p_1,p_2,\cdots,p_k$是不同的素数,$r_1,r_2,\cdots,r_k$ 和$s_1,s_2,\cdots,s_k$ 是非负整数),则

$$\gcd(m,n) = p_1^{\min(r_1,s_1)} p_2^{\min(r_2,s_2)} \cdots p_k^{\min(r_k,s_k)},$$

$$\mathrm{lcm}(m,n) = p_1^{\max(r_1,s_1)} p_2^{\max(r_2,s_2)} \cdots p_k^{\max(r_k,s_k)}.$$

下面介绍求两个正整数 m 和 n 的最大公因数 $\gcd(m, n)$的辗转相除法,又称为**欧几里得**(Euclid)**算法**,那是在公元前 300 年欧几里得在其《几何原本》中给出的,这可以算是离散数学最早的研究成果.

多次使用带余除法,有 $m=q_1n+r_1$,$0<r_1<n$,$n=q_2r_1+r_2$,$0<r_2<r_1$,$\cdots$,$r_{k-2}=q_{k-1}r_{k-1}+r_k$,$0<r_k<r_{k-1}$,$r_{k-1}=q_kr_k$,由于$\cdots<r_2<r_1<n$,这种 k 是存在的,于是 $\gcd(m, n)=\gcd(n, r_1)=\gcd(r_1, r_2)=\cdots=\gcd(r_{k-1}, r_k)=r_k$. 进而 $r_k=r_{k-2}-q_{k-1}r_{k-1}$,$\cdots$,$r_2=n-q_2r_1$,$r_1=m-q_1n$,于是存在整数 x 和 y 使得

$$\gcd(m,n) = mx + ny.$$

【例 1-19】 利用欧几里得算法计算 $\gcd(119, 35)$,并求出整数 x 和 y 使得 $\gcd(119, 35)=119x+35y$.

解 因为 $119=3\times 35+14$, $35=2\times 14+7$, $14=2\times 7$, 所以 $\gcd(119, 35)=7$. 由于 $7=35-2\times 14$,$14=119-3\times 35$, 于是 $7=35-2\times(119-3\times 35)=119\times(-2)+35\times 7$.

若 $\gcd(m, n)=1$,则称 m 和 n **互素**(coprime). 根据前面的讨论,$\gcd(m, n)=1$ 当且仅当存在整数 x 和 y 使得 $mx+ny=1$.

对于正整数 n,用 $\varphi(n)$表示小于等于 n 且与 n 互素的正整数个数,称 $\varphi(n)$为**欧拉函数**(Euler function). 例如 $\varphi(1)=1$,$\varphi(2)=1$,$\varphi(3)=2$,$\varphi(4)=2$,$\varphi(5)=4$,$\varphi(6)=2$. 当 p 为素数时,$\varphi(p)=p-1$.

设 n 是大于 1 的正整数 n,其素数分解为 $n=p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$,其中 $p_1,p_2,\cdots,p_k$是不同的素

数，$r_1, r_2, \cdots, r_k$是正整数，利用容斥原理（见下节）可以证明

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).$$

运算符号的选取 从运算的定义知道，运算本质上就是函数，只是在不同场合有不同称呼，所以，函数符号是运算符号；对于常见的运算，如数的加法运算，减法运算等，如果未加特殊说明，其运算的含义最好不要改变；实际上，运算符号可以自己规定，如“$*$”、“$\otimes$”、“$\oplus$”、“$\triangle$”、“&”、“□”、“:”、“|”、“•”、“$\odot$”、“$\cup$”、“$\circ$”、“♣”、“♦”、“♥”、“♠”等，但要把运算的含义定义清楚. 实际上，在C语言中出现了很多的运算符号.

运算符号的位置 运算符号，可以照函数符号一样，放在最前面；也可以放在最后；也可以放在中间，特别是2元运算符号，按照习惯，都写在中间位置；对于1元运算通常将运算符号前置$\neg x$、顶置$\bar{x}$或肩置x'. C语言中唯一的3元运算“条件运算”符为“？:”，其书写形式为x ? a : b，它也是将参加运算的3个对象分别写在第一、第二及第三位置. 数字逻辑中的与或非门是一个4元运算，有其独特的运算符号$\overline{AB+CD}$.

运算表 如果集合$A=\{x_1, x_2, \cdots, x_n\}$，则$A$上的1元或2元运算可以用一个表格表示出来. 如$A$上的2元运算$*$可以表示为表1-1.

例如，对于集合$A=\{a,b,c\}$，A上的$*$运算可以如表1-2定义.

表 1-1

$*$	x_1 ⋯ x_j ⋯ x_n
x_1 ⋮ x_i ⋮ x_n	⋯⋯ $x_i * x_j$

表 1-2

$*$	a	b	c
a	b	a	c
b	b	c	c
c	c	a	b

1.3.2 运算的性质

之所以讨论运算的性质，是为了便于根据运算的性质对离散数学结构进行分类，特别是在讨论代数结构的时候. 正因为这样，下面假定涉及的运算是根据问题需要定义出来的代数运算，这也是为讨论运算的结合性以及分配性提供方便.

1. 对合（involutive）性

【定义1-15】 设$*$是A上的1元代数运算，若对于任意的$x\in A$，均有

$$*(*x) = x \tag{1}$$

则称$*$具有**对合性**，或称$*$满足**对合律**.

【例1-20】 实数集上的取相反数运算“$-$”具有对合性，而其上的绝对值运算$|\ |$不具有对合性. 矩阵的逆运算及转置运算具有对合性，因为$(\mathbf{A}^{-1})^{-1}=\mathbf{A}$且$(\mathbf{A}^{\mathrm{T}})^{\mathrm{T}}=\mathbf{A}$.

2. 幂等（idempotent）性

【定义1-16】 设$*$是A上的2元代数运算，若对于$x\in A$有

$$x * x = x \tag{2}$$

则称x为关于$*$运算的**幂等元**（idempotent element）；若对于任意的$x\in A$，x均为幂等元，

则称 * 具有**幂等性**,或称 * 满足**幂等律**.

表 1-3

*	1	2	3
1	1	3	2
2	2	3	2
3	3	1	3

【例 1-21】 设 $A=\{1,2,3\}$,A 上的 * 运算见表 1-3.从运算表容易知道,1 和 3 是关于 * 运算的幂等元,但因为 2 不是幂等元,因此 * 运算不具有幂等性.

【例 1-22】 正整数集合 $\mathbf{N}^+$ 上的 gcd 及 lcm 运算均具有幂等性,因为对于任意正整数 x,均有 $\gcd(x,x)=x$,$\mathrm{lcm}(x,x)=x$.但对于实数集合 $\mathbf{R}$ 上的乘法运算来说,只有 0 和 1 是幂等元,从而 $\mathbf{R}$ 上的乘法运算不具有幂等性.

3. 交换(commutative)性

【定义 1-17】 设 * 是 A 上的 2 元代数运算,若对于任意的 $x,y\in A$,均有

$$x*y=y*x \tag{3}$$

则称 * 具有**交换性**,或称 * 满足**交换律**.

【例 1-23】 整数集合 $\mathbf{Z}$ 上的加法运算"+"满足交换律,而 $\mathbf{Z}$ 上的减法运算"−"不满足交换律,试验证.

解 显然,+具有交换性.取 $2,3\in\mathbf{Z}$,因为 $3-2\neq 2-3$,所以,−不具有交换性.

【例 1-24】 设 * 是有理数集合 $\mathbf{Q}$ 上的 2 元运算,定义如下:任意 $x_1,x_2\in\mathbf{Q}$,$x_1*x_2=x_1^{x_2}$.证明 * 不具有交换性.

证 取 $x=2,y=3$,这时,$x*y=2^3=8$,而 $y*x=3^2=9$,从而 * 不具有交换性.

由 1.2 节知,一般地说 $f\circ g\neq g\circ f$,所以映射的复合运算不满足交换律.

4. 结合(associative)性

【定义 1-18】 设 * 是 A 上的 2 元代数运算,若对于任意的 $x,y,z\in A$,均有

$$(x*y)*z=x*(y*z) \tag{4}$$

则称 * 具有**结合性**,或称 * 满足**结合律**.

【例 1-25】 试验证:整数集合 $\mathbf{Z}$ 上的加法运算+满足结合律,而 $\mathbf{Z}$ 上的减法运算−不满足结合律.

解 显然,+具有结合性.取 $2,3,5\in\mathbf{Z}$,因为 $(2-3)-5\neq 2-(3-5)$,所以,−不具有结合性.

【例 1-26】 根据表 1-4 的运算表,分别判定集合 $A=\{1,2,3,4,5\}$上定义的 * 运算是否满足交换律、结合律.

表 1-4

*	1	2	3	4	5
1	1	2	3	4	5
2	2	4	1	3	4
3	3	1	2	1	2
4	4	1	3	4	3
5	5	4	1	3	5

解 因为 $2*4=3\neq 1=4*2$,由此可见,* 不具有交换性.又由于 $(2*3)*4=4\neq 2=2*(3*4)$,所以,* 不具有结合性.

从运算表判定运算是否满足交换律,只需检查运算表是否关于主对角线对称.而从运算表判定运算是否满足结合律就困难一些.

注意 若运算满足结合律,则多个元素参加运算可不加括号.

5. 幺元律

【定义 1-19】 设 $*$ 是 A 上的 2 元代数运算，若存在 $e \in A$，对于任意的 $x \in A$，下列条件均成立：

$$e * x = x (\text{left identity element}) \tag{5}$$

$$x * e = x (\text{right identity element}) \tag{6}$$

则称 e 为集合 A 关于 $*$ 运算的**幺元素**或**单位元素**或称 $*$ 运算满足**幺元律**.

【例 1-27】 试验证：整数集合 $\mathbf{Z}$ 关于加法运算 $+$ 的单位元素为 0，而 $\mathbf{Z}$ 关于乘法运算"$\cdot$"的单位元素为 1，$\mathbf{Z}$ 关于减法运算 $-$ 没有单位元素.

解 对任意 $x \in \mathbf{Z}$，$0+x=x=x+0$ 及 $1 \cdot x=x=x \cdot 1$ 成立，所以，$\mathbf{Z}$ 关于加法运算 $+$ 的单位元素为 0，而 $\mathbf{Z}$ 关于乘法运算 $\cdot$ 的单位元素为 1. 因为 $x-e=x=e-x$ 对任意 x 都成立的元素 e 在 $\mathbf{Z}$ 中不存在，因此 $\mathbf{Z}$ 关于减法运算没有单位元素.

集合 A 关于 $*$ 运算的单位元素可记为 1，为避免与数 1 混淆，将单位元素记为 e.

【定理 1-13】 若 A 关于 $*$ 运算的有单位元素，则单位元素是唯一的.

证 设 e_1 和 e_2 是 A 关于 $*$ 运算的单位元素，则有 $e_1=e_1 * e_2=e_2$.

6. 零元律

【定义 1-20】 设 $*$ 是 A 上的 2 元代数运算，若存在 $\theta \in A$，对于任意的 $x \in A$，下列条件均成立：

$$\theta * x = \theta (\text{left zero element}) \tag{7}$$

$$x * \theta = \theta (\text{right zero element}) \tag{8}$$

则称 θ 为集合 A 关于 $*$ 运算的**零元素**或称 $*$ 运算满足**零元律**.

【例 1-28】 试验证：整数集合 $\mathbf{Z}$ 关于加法运算 $+$ 和减法运算 $-$ 均没有零元素，而 $\mathbf{Z}$ 关于乘法运算 $\cdot$ 的零元素为 0.

解 （作为练习）.

集合 A 关于 $*$ 运算的零元素可记为 0，为避免与数 0 混淆，将零元素记为 θ.

【定理 1-14】 若 A 关于 $*$ 运算的有零元素，则零元素是唯一的.

证（略）.

7. 逆元性

若 A 关于 $*$ 运算有单位元素 e，则可以讨论 A 中取定的元素 x 是否有逆元.

【定义 1-21】 设 $*$ 是 A 上的 2 元代数运算且有单位元素 e，若对于 $x \in A$，存在 $y \in A$，使得下列条件均成立：

$$y * x = e (\text{left invertible element}) \tag{9}$$

$$x * y = e (\text{right invertible element}) \tag{10}$$

则称 y 为 x 的**逆元素**或称 x 关于运算 $*$ 具有**逆元性**.

显然，一个方阵关于乘法运算的逆元就是其逆矩阵，因为单位元素是单位矩阵. 对于函数来说，一个映射关于函数的复合运算$\circ$的逆元就是其逆映射，当然只有双射才有逆元，其单位元素是恒等映射.

【例 1-29】 分别考察：实数集合 $\mathbf{R}$ 中各元素关于加法运算 $+$ 和乘法运算 $\cdot$ 的逆元素.

解 (1) $\mathbf{R}$ 关于加法运算 $+$ 的单位元素是 0. 对于任意 $x \in \mathbf{R}$，取 $y=-x$，因为 $x+(-x)=0=(-x)+x$，于是 $\mathbf{R}$ 中任意元素 x 均存在逆元 $-x$.

(2) $\mathbf{R}$ 关于乘法运算 · 的单位元素是 1. 对于任意 $x\in\mathbf{R}$,若 $x\neq 0$,取 $y=1/x$,因为 $x\cdot 1/x=1=1/x\cdot x$,于是非零元素 x 均存在逆元 $1/x$;若 $x=0$,显然不存在任何 $y\in\mathbf{R}$,满足条件 $0\cdot y=1$,从而 0 关于乘法无逆元素.

【例 1-30】 设 $A=\{a,b,c\}$关于 $*$ 运算的运算表如表 1-5 所示.

表 1-5

$*$	a	b	c
a	a	b	c
b	b	a	a
c	c	a	c

由表 1-5 可知,a 是 $A=\{a,b,c\}$关于 $*$ 运算的单位元素. 因为 $b*b=a$ 且 $b*c=c*b=a$,所以 b,c 都是 b 的逆元.

对于 $\mathbf{Z}_6=\{0, 1, 2, 3, 4, 5\}$中的模 6 乘法运算"$\cdot_6$"来说,由于 1 是该运算的单位元素,容易验证关于"$\cdot_6$"运算 1 和 5 有逆元,分别为 1 和 5,而 2, 3 和 4 不存在逆元. 对于模 6 加法运算"$+_6$"来说,由于 0 是该运算的单位元素,容易验证 $\mathbf{Z}_6=\{0, 1, 2, 3, 4, 5\}$中的每个元素关于"$+_6$"运算均有逆元,分别为 0, 5, 4, 3, 2, 1.

由上面的例子可知,一个元素的逆元不一定存在,即使存在也不一定唯一. 但有下面的结论.

【定理 1-15】 设 A 关于 $*$ 运算的单位元素为 e 且 $*$ 运算满足结合律,若 $x\in A$ 在 A 中有左逆元 y 及右逆元 z,则 $y=z$. 进而,对于一个满足结合律的运算来说,若一个元素有逆元则其逆元是唯一的.

证 由已知条件有,$y*x=e$ 且 $x*z=e$. 于是,

$$y = y*e = y*(x*z) = (y*x)*z = e*z = z$$

若元素 $x\in A$ 有唯一逆元,则将其记为 x^{-1}.

8. 消去(cancellation)性

【定义 1-22】 设 $*$ 是 A 上的 2 元代数运算,若 A 关于 $*$ 运算有零元则记为 θ,如果对于任意的 $x,y,z\in A$,只要 $x\neq\theta$,那么下列条件均成立:

由 $x*y=x*z$ 可推出

$$y = z(\text{left cancellation property}) \tag{11}$$

由 $y*x=z*x$ 可推出

$$y = z(\text{right cancellation property}) \tag{12}$$

则称 $*$ 具有**消去性**,或称 $*$ 满足**消去律**.

【例 1-31】 试验证:整数集合 $\mathbf{Z}$ 上的加法运算$+$和乘法运算 · 均满足消去律.

证 注意,$+$和 · 满足交换性,只需验证(1)即可. 对于任意 $x,y,z\in\mathbf{Z}$,若 $x+y=x+z$,有 $y=z$ 成立,所以,$+$具有消去性. 同样,因为 $\mathbf{Z}$ 关于乘法运算的零元为 0,而对于任意取 $x,y,z\in\mathbf{Z}$,若 $x\neq 0$,则由 $x\cdot y=x\cdot z$ 显然可推出 $y=z$,因此,· 具有消去性.

【例 1-32】 试说明对于实数集 $\mathbf{R}$ 上的所有 2 阶方阵组成的集合 $\boldsymbol{M}_2(\mathbf{R})$,其上的矩阵乘法运算不满足消去律.

解 因为 A 关于矩阵乘法运算的零元是$\begin{pmatrix}0&0\\0&0\end{pmatrix}$,取 $x=\begin{pmatrix}1&0\\0&0\end{pmatrix}\neq\begin{pmatrix}0&0\\0&0\end{pmatrix}$,由于$\begin{pmatrix}1&0\\0&0\end{pmatrix}\cdot\begin{pmatrix}0&0\\1&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}=\begin{pmatrix}1&0\\0&0\end{pmatrix}\cdot\begin{pmatrix}0&0\\1&1\end{pmatrix}$,而$\begin{pmatrix}0&0\\1&0\end{pmatrix}\neq\begin{pmatrix}0&0\\1&1\end{pmatrix}$,所以 $\boldsymbol{M}_2(\mathbf{R})$上的乘法运算不满足消去律.

9. 分配(distributive)性

【定义 1-23】 设 $*$ 和 $\circ$ 是集合 A 上的两个 2 元代数运算,若对于任意 $x,y,z\in A$,有

$$x*(y\circ z)=(x*y)\circ(x*z)\text{(left distributive property)} \tag{13}$$

$$(y\circ z)*x=(y*x)\circ(z*x)\text{(right distributive property)} \tag{14}$$

则称 $*$ 运算对 $\circ$ 运算**可分配**.

【例 1-33】 实数集合 **R** 上的乘法运算 $\cdot$ 对加法运算 $+$ 可分配,但加法运算 $+$ 对乘法运算 $\cdot$ 不可分配.

解 对于任意的 $x,y,z\in\mathbf{R}$,有 $x\cdot(y+z)=(x\cdot y)+(x\cdot z)$ 且 $(y+z)\cdot x=(y\cdot x)+(z\cdot x)$,于是乘法运算 $\cdot$ 对加法运算 $+$ 可分配. 因为 $2+(3\cdot 5)\neq(2+3)\cdot(2+5)$,因此,加法运算 $+$ 对乘法运算 $\cdot$ 不可分配.

注意 当 $*$ 运算满足交换性时,式(13)和式(14)之一成立即可.

【例 1-34】 设 $\mathbf{R}[x]$ 表示实数集 **R** 上的所有关于 x 的一元多项式组成的集合,试验证:多项式的乘法运算对多项式的加法运算可分配.

解 (作为练习).

【例 1-35】 设 $\boldsymbol{M}_n(\mathbf{R})$ 表示实数集 **R** 上的所有 n 阶方阵组成的集合,试验证:矩阵的乘法运算对矩阵的加法运算可分配.

解 (作为练习).

10. 吸收(absorptive)性

【定义 1-24】 设 $*$,$\circ$ 是集合 A 上的两个 2 元代数运算,若对于任意 $x,y\in A$,有

$$x*(x\circ y)=x\text{(left absorptive property)} \tag{15}$$

$$(x\circ y)*x=x\text{(right absorptive property)} \tag{16}$$

则称 $*$ 运算对 $\circ$ 运算**可吸收**.

如果 $*$ 和 $\circ$ 是集合 A 上的两个可交换的 2 元代数运算,则 $*$ 运算对 $\circ$ 运算可吸收只需要满足式(15)或式(16)即可,但吸收性本身不需要 $*$ 和 $\circ$ 可交换.

【例 1-36】 实数集合 **R** 上的乘法运算 $\cdot$ 对加法运算 $+$ 不可吸收,因为不满足对于任意 $x,y\in\mathbf{R}$,有 $x\cdot(x+y)=x$.

11. 德·摩根(De Morgan, 1806—1871)律

【定义 1-25】 设 $\bullet$ 是集合 A 上的 1 元代数运算,$*$ 和 $\circ$ 是 A 上的两个 2 元代数运算,若对于任意 $x,y\in A$,均有下面两个等式成立

$$\bullet(x*y)=(\bullet x)\circ(\bullet y) \tag{17}$$

$$\bullet(x\circ y)=(\bullet x)*(\bullet y) \tag{18}$$

则称这三种运算满足 **De Morgan 律**.

【例 1-37】 非负实数集合上的开算术平方根运算,与其上的加法运算、乘法运算不满足 De Morgan 律,因为对于某些 $x,y\in\mathbf{R}$,有 $\sqrt{x\cdot y}\neq\sqrt{x}+\sqrt{y}$.

人们已经知道了运算可能具有的常见性质,在特定的数学结构中,还会出现一些别的运算性质,如**定理 2-3** 中的结论,在此不一一列举了.

上面介绍了运算的定义及性质. 在实际应用中,可能会有几种运算同时出现的情况,这时请注意括号的添加,当然为了方便起见可以约定运算的顺序,参见有关的 C 程序设计语言教材[3].

习　题　1.3

1. 分别判定取绝对值运算‖、加法运算+、减法运算−、取大运算 max、取小运算 min 是否为自然数集合 **N** 上的代数运算.

2. 证明：集合 $A=\{3^n \mid n\in \mathbf{N}\}$关于数的加法运算不封闭.

3. 设 $A=\{a,b,c\}$,求出 A 上的 2 元代数运算的个数.

4. 将十进制数 365 转换成八进制.

5. 分别计算 16(mod 3),−16(mod 3),0(mod 3).

6. 利用素因数分解计算 gcd(36, 48)和 lcm(36, 48).

7. 使用欧几里得算法,计算 gcd(14, 158) 并求出整数 x 和 y 使得 $\gcd(14, 158)=14x+158y$.

8. 设 $A=\{1,2,3\}$,试根据所给定的运算表 1-6 和表 1-7 分别讨论其幂等性、交换性以及是否有单位元素,若有,请指出 A 中各元素的逆元素.

表　1-6

*	1	2	3
1	1	2	3
2	2	2	3
3	3	3	2

表　1-7

*	1	2	3
1	1	2	3
2	2	2	2
3	3	1	3

9. 整数集合 **Z** 上的取大运算 max 和取小运算 min 相互可吸收. 试证明之.

10. 设 $\mathbf{R}[x]$表示实数集 **R** 上的所有关于 x 的一元多项式组成的集合,试验证：

(1) 多项式的加法运算和多项式的乘法运算均满足结合律；

(2) 多项式的乘法运算对多项式的加法运算可分配.

11. 设 $\boldsymbol{M}_n(\mathbf{R})$表示实数集 **R** 上的所有 n 阶方阵组成的集合.

(1) 试验证:矩阵的乘法运算对矩阵的加法运算可分配.

(2) $\boldsymbol{M}_n(\mathbf{R})$关于矩阵乘法的单位元素是什么? $\boldsymbol{M}_n(\mathbf{R})$中哪些元素关于乘法运算有逆元?

12. 令 $\mathbf{Z}_m=\{0,1,2,\cdots,m-1\}$,$\mathbf{Z}_m$上的两个 2 元运算分别是模 m 的加法运算“$+_m$”和模 m 的乘法运算“$\cdot_m$”,定义如下：任意 $x,y\in \mathbf{Z}_m$,$x+_m y=(x+y) \bmod m$,$x\cdot_m y=(xy) \bmod m$.

(1) 写出 $\mathbf{Z}_6$关于$+_6$和$\cdot_6$的运算表.

(2) 证明：$\cdot_m$运算对$+_m$运算可分配.

13. 试验证：**Z** 关于加法运算+和减法运算−均没有零元素，而 **Z** 关于乘法运算“·”的零元素为 0.

14. 试举例说明,映射的复合运算“∘”不具有消去性.

15. 令 G 表示集合 $S=\{1,2,3\}$上所有置换组成的集合.

(1) 列出 G 关于复合映射“∘”的运算表.

(2) 指出 G 关于复合映射“∘”的单位元素及 G 中每个元素的逆元.

1.4　集合的运算

最常见的集合运算是并运算、交运算和补运算.

1.4.1　并运算

【定义 1-26】 设 A 和 B 是集合,则 A 和 B 的**并集**(union)$A\cup B$ 定义如下:

$$A\cup B=\{x\mid x\in A \text{ 或 } x\in B\}$$

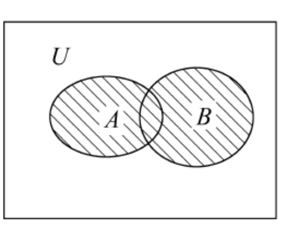


图　1-8

集合 $A\cup B$ 就是将集合 A 与 B 中元素全部取出来构成的集合,也可以说为 $A+B$,在文氏图中的表示是图 1-8 中的阴影部分.

显然,集合的并运算是 $P(U)$ 上的 2 元封闭运算,即 $\cup$:$P(U)\times P(U)\rightarrow P(U)$,在不强调运算所依赖的集合 $P(U)$ 时,就说成是集合的并运算,这是大家所默认的.

【定理 1-16】 设 A 和 B 是集合,则 $A\cup B$ 是包含集合 A 和集合 B 的最小集合.

证　显然,$A\cup B\supseteq A$ 且 $A\cup B\supseteq B$. 令 C 是任意一个包含 A 和 B 的集合,即 $C\supseteq A$,$C\supseteq B$,这时有 $C\supseteq A\cup B$,也就是说 $A\cup B$ 比 C"小".

显然,有下列结论:

【定理 1-17】 设 A,B,C 是集合,则

(1) $A\cup A=A$(**幂等律**);

(2) $A\cup B=B\cup A$(**交换律**);

(3) $(A\cup B)\cup C=A\cup(B\cup C)$(**结合律**);

(4) $A\cup\varnothing=\varnothing\cup A=A$(空集$\varnothing$是并运算$\cup$的**单位元**);

(5) $A\cup U=U\cup A=U$ (全集 U 是并运算$\cup$的**零元素**).

两个集合的并运算可以推广到更多个集合的并运算. 设 $A_i(1\leqslant i\leqslant n)$是集合,则

$$\bigcup_{i=1}^{n}A_i=A_1\cup A_2\cup\cdots\cup A_n=\{x\mid x\in A_1,\text{或 } x\in A_2,\cdots,\text{或 } x\in A_n\}$$

还可以推广到更一般的情形 $\bigcup\limits_{i\in I}A_i$,其中 I 是指标集,如 $\bigcup\limits_{i=1}^{\infty}A_i$.

【例 1-38】 设 f:$A\rightarrow B$,对于任意 $X\subseteq A$,$Y\subseteq A$,证明:$f(X\cup Y)=f(X)\cup f(Y)$.

证　因为 $X\subseteq X\cup Y$,显然有 $f(X)\subseteq f(X\cup Y)$,同样道理,$f(Y)\subseteq f(X\cup Y)$,进而有 $f(X)\cup f(Y)\subseteq f(X\cup Y)$. 下面证明:$f(X\cup Y)\subseteq f(X)\cup f(Y)$.

对于任意 $b\in f(X\cup Y)$,必存在 $a\in X\cup Y$,使得 $b=f(a)$. 这时,$a\in X$ 或 $a\in Y$. 若 $a\in X$,则 $b=f(a)\in f(X)$;若 $a\in Y$,则 $b=f(a)\in f(Y)$. 因此,$b\in f(X)\cup f(Y)$. 于是,$f(X\cup Y)\subseteq f(X)\cup f(Y)$.

由 1.1 节定理 1-3 知,$f(X\cup Y)=f(X)\cup f(Y)$.

1.4.2　交运算

【定义 1-27】 设 A 和 B 是集合,则 A 和 B 的**交集**(intersection)$A\cap B$ 定义如下:

$$A\cap B=\{x\mid x\in A \text{ 且 } x\in B\}$$

集合 $A\cap B$ 就是将集合 A 与 B 中所有公共元素取出来构成的集合，也可以记为 $A\cdot B$ 或 AB，在文氏图中的表示是图 1-9 中的阴影部分.

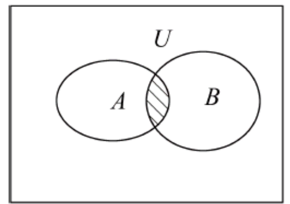
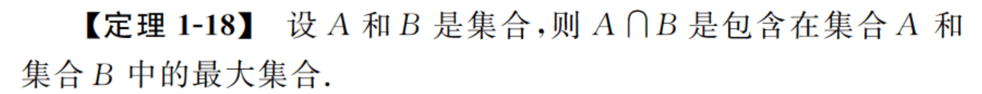


图 1-9

【例 1-39】 设集合 $\pi_1=\{\{1,4\},\{2,3\}\}$，$\pi_2=\{\{1\},\{2,3,4\}\}$，计算集合 $\pi=\{X\mid X$ 非空，且 $X=A\cap B,A\in\pi_1,B\in\pi_2\}$.

解 $\pi=\{\{1\},\{4\},\{2,3\}\}$.

可以证明：



【定理 1-18】 设 A 和 B 是集合，则 $A\cap B$ 是包含在集合 A 和集合 B 中的最大集合.

证 显然，$A\cap B\subseteq A$ 且 $A\cap B\subseteq B$. 令 C 是任意一个包含在 A 和 B 的集合，即 $C\subseteq A$，$C\subseteq B$，这时有 $C\subseteq A\cap B$，也就是说 $A\cap B$ 比 C"大".

显然，有下列结果：

【定理 1-19】 设 A,B,C 是集合，则

(1) $A\cap A=A$(**幂等律**).

(2) $A\cap B=B\cap A$(**交换律**).

(3) $(A\cap B)\cap C=A\cap(B\cap C)$(**结合律**).

(4) $A\cap U=U\cap A=A$(全集 U 是交运算 $\cap$ 的**单位元素**).

(5) $A\cap\varnothing=\varnothing\cap A=\varnothing$(空集 $\varnothing$ 是交运算 $\cap$ 的**零元素**).

两个集合的交运算可以推广到更多个集合的交运算. 设 $A_i(1\leqslant i\leqslant n)$ 是集合，则

$$\bigcap_{i=1}^{n}A_i=A_1\cap A_2\cap\cdots\cap A_n=\{x\mid x\in A_1,\text{且 }x\in A_2,\cdots,\text{且 }x\in A_n\}$$

还可以推广到更一般的情形 $\bigcap_{i\in I}A_i$，其中 I 是指标集.

【例 1-40】 设 $f:A\to B$，对于任意 $X\subseteq A,Y\subseteq A$，判定 $f(X\cap Y)=f(X)\cap f(Y)$ 是否成立，说明理由.

解 (作为练习).

下面的定理讨论的是并运算与交运算之间所满足的性质.

【定理 1-20】 设 A,B,C 是集合，则

(1) $\begin{cases}A\cap(A\cup B)=A(\cap\text{对}\cup\text{可吸收})\\A\cup(A\cap B)=A(\cup\text{对}\cap\text{可吸收})\end{cases}$

(2) $\begin{cases}A\cap(B\cup C)=(A\cap B)\cup(A\cap C)(\cap\text{对}\cup\text{可分配})\\A\cup(B\cap C)=(A\cup B)\cap(A\cup C)(\cup\text{对}\cap\text{可分配})\end{cases}$

【例 1-41】 对于集合 A,B，证明下列 3 个命题等价：

(1) $A\subseteq B$；

(2) $A\cap B=A$；

(3) $A\cup B=B$.

证 由(1)推(2)：显然有 $A\cap B\subseteq A$. 对于任意 $x\in A$，由已知条件 $A\subseteq B$，有 $x\in B$，进而 $x\in A\cap B$，于是 $A\subseteq A\cap B$. 因此，$A\cap B=A$.

由(2)推(1)：因为 $A\cap B\subseteq B$，而已知 $A\cap B=A$，所以 $A\subseteq B$.

类似地可以证明(1)与(3)等价.

1.4.3 补运算

【定义 1-28】 设 U 是全集，对于集合 A，定义 A 的**补集**(complement)$\overline{A}$ 如下：

$$\overline{A}=\{x \mid x\in U,\text{但 } x\notin A\}$$

由补运算的定义可知，一个集合的补集依赖于全集的选取.

【例 1-42】 设集合 $A=\{a,b,c\}$，分别取全集 $U=\{a,b,c,d\}$ 和 $U=\{a,b,c,\{a,b\},\{b,c\},\{\{c\}\}\}$，求 $\overline{A}$.

解 若 $U=\{a,b,c,d\}$，则 $\overline{A}=\{d\}$；若 $U=\{a,b,c,\{a,b\},\{b,c\},\{\{c\}\}\}$，则 $\overline{A}=\{\{a,b\},\{b,c\}.\{\{c\}\}\}$.

求 A 的补集符号 $\overline{A}$ 是由罗素等人大约在 1900 年引入的，集合 $\overline{A}$ 在文氏图中的表示如图 1-10 中的阴影部分.

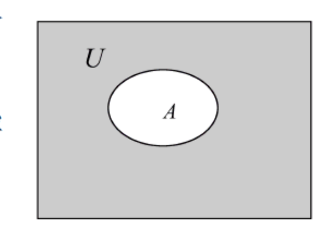


图 1-10

显然，补运算具有对合性：$\overline{\overline{A}}=A$. 下面的定理是重要的，它是经典集合特有的一条性质，称为**排中律**.

【定理 1-21】 设 A 是集合，则 A 的补集 $\overline{A}$ 满足：

(1) $A\cup\overline{A}=U$；

(2) $A\cap\overline{A}=\varnothing$.

结合图 1-10 很容易理解上述定理，它说明对于全集中的任意元素 x，$x\notin A$ 当且仅当 $x\in\overline{A}$，即 $x\in A$ 或 $x\in\overline{A}$ 必居其一，只能具有“非此即彼”二元性，不具有“亦此亦彼”中间过渡性.

集合的补运算和集合的并交运算满足 De Morgan 律.

【定理 1-22】 设 A，B 是集合，则：

(1) $\overline{A\cup B}=\overline{A}\cap\overline{B}$；

(2) $\overline{A\cap B}=\overline{A}\cup\overline{B}$.

证 (作为练习).

有些与整数 n 有关的结论的证明可以使用数学归纳法，其有效性是显然的.

第一数学归纳法(first mathematical induction) 设 n_0 是整数[①]，给定一个关于整数 $n\geqslant n_0$ 的命题 $P(n)$，若

(1) **归纳基础** $P(n_0)$成立.

(2) **归纳步骤** 对任意的 $n>n_0$，由 $P(n-1)$成立可以得出 $P(n)$成立.

则对于任意 $n\geqslant n_0$ 均有 $P(n)$成立.

第二数学归纳法(second mathematical induction) 设 n_0 是整数，给定一个关于整数 $n\geqslant n_0$ 的命题 $P(n)$，若

(1) **归纳基础** $P(n_0)$成立.

(2) **归纳步骤** 对任意的 $n>n_0$，由 $P(n_0)$、$P(n_0+1)$、…、$P(n-1)$成立可以得出 $P(n)$成立，则对于任意 $n\geqslant n_0$ 均有 $P(n)$成立.

推广的 De Morgan 律 设 $A_1,A_2,\cdots,A_n$ 是集合，则

(1) $\overline{A_1\cup A_2\cup\cdots\cup A_n}=\overline{A_1}\cap\overline{A_2}\cap\cdots\cap\overline{A_n}$.

---

① 很多时候 $n_0=1$.

(2) $\overline{A_1 \cap A_2 \cap \cdots \cap A_n} = \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_n}$.

证 (1) 对 n 使用数学归纳法. 当 $n=2$ 时,结论显然成立. 假设 $n-1$ 时结论成立,由于

$$\begin{aligned}\overline{A_1 \cup A_2 \cup \cdots \cup A_n} &= \overline{(A_1 \cup A_2 \cup \cdots \cup A_{n-1}) \cup A_n} \\ &= \overline{(A_1 \cup A_2 \cup \cdots \cup A_{n-1})} \cap \overline{A_n} \\ &= (\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_{n-1}}) \cap \overline{A_n} \\ &= \overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}.\end{aligned}$$

(2) (留作练习)

集合的 $\cup$, $\cap$, $\bar{}$ 运算的重要性质列举如下:

(1) $\overline{\overline{A}} = A$(对合律);

(2) $A \cup A = A$, $A \cap A = A$ (幂等律);

(3) $A \cup B = B \cup A$, $A \cap B = B \cap A$ (交换律);

(4) $(A \cup B) \cup C = A \cup (B \cup C)$, $(A \cap B) \cap C = A \cap (B \cap C)$ (结合律);

(5) $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$(吸收律);

(6) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$(分配律);

(7) $A \cup \overline{A} = U$, $A \cap \overline{A} = \varnothing$(有补律: A 有补元 $\overline{A}$);

(8) $\overline{A \cup B} = \overline{A} \cap \overline{B}$, $\overline{A \cap B} = \overline{A} \cup \overline{B}$(德·摩根律);

(9) $A \cup \varnothing = \varnothing \cup A = A$, $A \cap U = U \cap A = A$($\cup$, $\cap$ 有单位元);

(10) $A \cup U = U \cup A = U$, $A \cap \varnothing = \varnothing \cap A = \varnothing$($\cup$, $\cap$ 有零元).

上面列举的性质(7)可以称为有补律.

下面再介绍集合的差运算和对称差(环和)运算.

1.4.4 差运算

【定义 1-29】 集合 A,B 的**差集**(subtraction)定义如下:

$$A - B = \{x \mid x \in A \text{ 且 } x \notin B\}$$

集合 $A-B$ 就是从集合 A 中去掉属于 B 的元素,在文氏图中的表示是图 1-11 中的左边阴影,而右边阴影部分是 $B-A$.

【例 1-43】 设 $A=\{a,b,c\}$, $B=\{b,c,d,e,f\}$,分别计算 $A-B$ 和 $B-A$.

解 $A-B=\{a\}$, $B-A=\{d,e,f\}$.

显然,$A-B \neq B-A$,即集合的差运算不满足交换律. 对满足什么条件的集合 A,B,$A-B=B-A$ 成立,请大家思考.

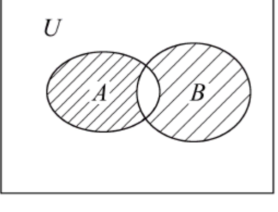


图 1-11

【例 1-44】 计算 $\mathbf{R}-\mathbf{Q}$,其中 $\mathbf{R}$ 是实数集合,$\mathbf{Q}$ 是有理数集合.

解 $\mathbf{R}-\mathbf{Q}=\{x \mid x \text{ 是无理数}\}$.

显然,$\overline{A}=U-A$. 鉴于补运算本身的特殊性,我们才单独讨论补运算. 下面的定理是有关差运算的重要结论.

【定理 1-23】 对于集合 A,B,有 $A-B=A\cap\overline{B}$.

证 (1) 先证明 $A-B \subseteq A\cap\overline{B}$:任意 $x \in A-B$,根据差运算的定义知 $x \in A$ 且 $x \notin B$,这

时 $x \in A$ 且 $x \in \overline{B}$,于是 $x \in A \cap \overline{B}$,因此有 $A-B \subseteq A \cap \overline{B}$.

(2) 再证明 $A \cap \overline{B} \subseteq A-B$:任意 $x \in A \cap \overline{B}$,这时 $x \in A$ 且 $x \in \overline{B}$,于是 $x \in A$ 且 $x \notin B$,根据差运算的定义知 $x \in A-B$,所以有 $A \cap \overline{B} \subseteq A-B$.

由(1)和(2)知,$A-B=A \cap \overline{B}$.

利用上述定理,可以方便地证明一些与差运算有关的题目.

【例 1-45】 对于任意集合 A,B,C,证明:$(A-B)-C=A-(B \cup C)$.

证 $(A-B)-C=(A \cap \overline{B})-C=(A \cap \overline{B}) \cap \overline{C}=A \cap (\overline{B} \cap \overline{C})$

$$=A \cap \overline{B \cup C}=A-(B \cup C).$$

【例 1-46】 设 A,B 是集合,证明:$A \subseteq B$ 当且仅当 $A-B=\varnothing$.

证 (作为练习).

【例 1-47】 对于任意集合 A,B,C,找出使下列等式

$$(A-B) \cup (A-C)=\varnothing$$

成立的最简单的充要条件.

解 因为$(A-B) \cup (A-C)=(A \cap \overline{B}) \cup (A \cap \overline{C})= A \cap (\overline{B} \cup \overline{C})=A \cap \overline{B \cap C}=A-(B \cap C)$,由已知条件有 $A-(B \cap C)=\varnothing$. $A-(B \cap C)=\varnothing$的充要条件是 $A \subseteq B \cap C$.

1.4.5 对称差运算

【定义 1-30】 集合 A,B 的**对称差**(symmetric difference)定义如下:

$$A \oplus B=(A-B) \cup (B-A)$$

集合的对称差运算又可称为**环和**(cycle sum)运算,它是针对运算符号而言的.

集合 $A \oplus B$ 在文氏图中的表示是图 1-12 中的两个对称的差 $A-B$ 与 $B-A$ 的并.

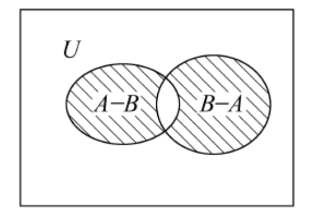


图 1-12

从文氏图容易看出

$$A \oplus B = (A \cup B) - (A \cap B)$$

【例 1-48】 设 $A=\{a,b,c\}$,$B=\{b,c,d,e,f\}$,计算 $A \oplus B$.

解 因为 $A-B=\{a\}$,$B-A=\{d,e,f\}$,所以 $A \oplus B=\{a,d,e,f\}$.

集合的对称差运算具有以下性质.

【定理 1-24】 对于集合 A,B,有:

(1) $A \oplus B=B \oplus A$;

(2) $A \oplus \varnothing=A$;

(3) $A \oplus A=\varnothing$;

(4) $(A \oplus B) \oplus C=A \oplus (B \oplus C)$.

证 (略).

【例 1-49】 对于任意集合 A,B,C,若 $A \oplus B=A \oplus C$,则 $B=C$,试证明之.

证 因为 $A \oplus B=A \oplus C$,所以 $A \oplus (A \oplus B)=A \oplus (A \oplus C)$. 由对称差运算的性质(4),有 $(A \oplus A) \oplus B=(A \oplus A) \oplus C$,再使用性质(3),有$\varnothing \oplus B=\varnothing \oplus C$. 最后由性质(2)得出$B=C$.

关于对称差运算的性质(3),我们有更进一步的结论.

【例 1-50】 设 A,B 是集合,证明:$A \oplus B=\varnothing$当且仅当 $A=B$.

证 若 $A=B$,则由性质(3)知 $A\oplus B=\varnothing$. 反过来,若 $A\oplus B=\varnothing$,因为 $A\oplus B=(A-B)\cup(B-A)$,所以 $A-B=\varnothing$,且 $B-A=\varnothing$,于是 $A\subseteq B$ 且 $B\subseteq A$,从而有 $A=B$.

可以考虑集合的交运算以及并运算与对称差运算之间的关系.

【例 1-51】 设 A,B,C 是集合,则

(1) $A\cap(B\oplus C)=(A\cap B)\oplus(A\cap C)$($\cap$对$\oplus$可分配).

(2) 举例说明 $A\cup(B\oplus C)=(A\cup B)\oplus(A\cup C)$不成立($\cup$对$\oplus$不可分配).

解 (留作练习).

思考 还能给出集合的其他运算吗?计算机如何做这些运算?

提示 $\overline{A\cup B},\overline{A\cap B},\overline{A-B},\overline{A\oplus B}$(部分参见习题 1.4 的第 11 题).

容斥原理(inclusion-exclusion principle)是加法原理的推广形式.

容斥原理 设 A,B 是有限集合,则 $|A\cup B|=|A|+|B|-|A\cap B|$.

该原理可以从文氏图直观理解,它的另一种形式是:

容斥原理的另一种形式 设 A,B 是有限集合,则

$$|\overline{A}\cap\overline{B}|=|U|-|A|-|B|+|A\cap B|$$

证 因为 $\overline{A}\cap\overline{B}=\overline{A\cup B}$,而 $|\overline{A\cup B}|=|U|-|A\cup B|$.

【例 1-52】 计算由 $1,2,3,\cdots,n(n\geqslant 4)$做成的 1 与 2 不相邻且 3 与 4 不相邻的全排列个数.

解 由 $1,2,3,\cdots,n(n\geqslant 4)$做成的全排列是全集 U. 显然,$|U|=n!$. 令 A,B 分别表示 U 中 1 与2 相邻,3 与 4 相邻的全排列组成的集合,则

$$|A|=|B|=2(n-1)!,|A\cap B|=4(n-2)!$$

而所求的满足条件的排列个数为$|\overline{A}\cap\overline{B}|$,于是有

$$\begin{aligned}|\overline{A}\cap\overline{B}|&=|U|-|A|-|B|+|A\cap B|=n!-2\cdot 2(n-1)!+4(n-2)!\\&=(n^2-5n+8)(n-2)!\end{aligned}$$

推广的容斥原理 设 $A_1,A_2,\cdots,A_n$ 是集合,则

$$\begin{aligned}|A_1\cup A_2\cup\cdots\cup A_n|=&\sum_{i=1}^{n}|A_i|-\sum_{1\leqslant i<j\leqslant n}|A_i\cap A_j|+\sum_{1\leqslant i<j<k\leqslant n}|A_i\cap A_j\cap A_k|\\&-\cdots+(-1)^{n+1}|A_1\cap A_2\cap\cdots\cap A_n|.\end{aligned}$$

由于$|\overline{A_1}\cap\overline{A_2}\cap\cdots\cap\overline{A_n}|=|\overline{A_1\cup A_2\cup\cdots\cup A_n}|$,于是有下述结论.

推广容斥原理的另一种形式 设 $A_1,A_2,\cdots,A_n$ 是集合,则

$$\begin{aligned}|\overline{A_1}\cap\overline{A_2}\cap\cdots\cap\overline{A_n}|=&|U|-\sum_{i=1}^{n}|A_i|+\sum_{1\leqslant i<j\leqslant n}|A_i\cap A_j|-\sum_{1\leqslant i<j<k\leqslant n}|A_i\cap A_j\cap A_k|\\&+\cdots+(-1)^{n}|A_1\cap A_2\cap\cdots\cap A_n|.\end{aligned}$$

习 题 1.4

1. 设全集 $U=\{a,b,c,d,e,f,g,h\}$,令集合 A,B,C,D 分别为 $A=\{a,b,c,g\}$,$B=\{d,e,f,g\}$,$C=\{a,c,f\}$,$D=\{f,h\}$. 分别计算(1)$A\cup B$;(2)$B\cap C$;(3)$A-D$;(4)$(A\cap B)-C$;(5)$\overline{D}$;(6)$B\oplus C$;(7)$A\cap(B\cup C)$;(8)$(A\cup D)-\overline{C}$;(9)$\overline{A\cup C}$;(10)$A\cup B\cup C$.

2. 设 $A\subseteq C$ 且 $B\subseteq C$,则 $A\cup B\subseteq C$,进而 $A\cap B\subseteq C$.

3. 证明德·摩根(De Morgan)律.

4. 对于集合 A,B,证明:$A\subseteq B$ 当且仅当 $\overline{B}\subseteq\overline{A}$.

5. 设 $f:A\to B$,对于任意 $X\subseteq A$ 及 $Y\subseteq A$,证明:$f(X\cap Y)\subseteq f(X)\cap f(Y)$. 一般来说,$f(X\cap Y)\neq f(X)\cap f(Y)$,举例说明之.

6. 对于任意集合 A,B,C,证明:$(A-B)-C=(A-C)-B$.

7. 设 A,B,C 是集合,下列命题是否成立,为什么?

(1) 若 $A\cup B=A\cup C$,则 $B=C$;

(2) 若 $A\cap B=A\cap C$,则 $B=C$;

(3) 若 $A\cup B=A\cup C$ 且 $A\cap B=A\cap C$,则 $B=C$.

8. 对于任意集合 A 和 B,证明:

(1) $P(A)\cap P(B)=P(A\cap B)$;

(2) $P(A)\cup P(B)\subseteq P(A\cup B)$,并举例说明 $P(A)\cup P(B)=P(A\cup B)$不成立.

9. 设 A,B 是集合,证明:$A\subseteq B$ 当且仅当 $A-B=\varnothing$.

10. 对于任意集合 A,B,C,分别找出使下列等式成立的最简单的充要条件:

(1) $(A-B)\cup(A-C)=A$;

(2) $(A-B)\cap(A-C)=\varnothing$;

(3) $(A-B)\oplus(A-C)=\varnothing$.

11. 设 A,B 是集合,定义$\otimes$(**环积**,cycle product)运算如下:

$$A\otimes B=\overline{A\oplus B}$$

证明:$A\otimes B=(A\cup\overline{B})\cap(\overline{A}\cup B)$,并讨论$\otimes$运算具有的性质.

12. 对于任意集合 A,B 和 C,证明:

(1) $A\cap(B\oplus C)=(A\cap B)\oplus(A\cap C)$;

(2) $(B\oplus C)\cap A=(B\cap A)\oplus(C\cap A)$.

13. 设 A,B,C 是集合,举例说明 $A\cup(B\oplus C)=(A\cup B)\oplus(A\cup C)$不成立.

14. 根据集合$\cup$和$\cap$相互可吸收证明$\cup$和$\cap$满足幂等性.

15. 设 A,B,C 是集合,利用两个集合的容斥原理证明:

$$\begin{aligned}|A\cup B\cup C|=&(|A|+|B|+|C|)\\&-(|A\cap B|+|A\cap C|+|B\cap C|)+|A\cap B\cap C|\end{aligned}$$

能推广到更一般的 n 个集合的情形吗?

16. (**错排问题**) 有 $1, 2, \cdots, n$ 共 n 个元素进行排列,若第 i 个元素都没有排在第 i 位置($i=1, 2, \cdots, n$),称这样的排列为**错排**(derangement). 利用 n 个集合的容斥原理计算错排的个数.

17. (**Euler 函数**) 对于大于 1 的正整数 n,若 $n=p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$,其中 $p_1,p_2,\cdots,p_k$是不同的素数,$r_1,r_2,\cdots,r_k$是正整数,则

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).$$

1.5 集合的划分与覆盖

集合的划分就是集合元素间的一种分类. 在信息科学中,对知识库分类就是集合的一种

划分.因此,研究集合的划分具有特别重要的意义.比集合的划分更广的概念是集合的覆盖.这些内容在下章会用到.

1.5.1 集合的划分

硬盘分区、实验分组以及各种分类等都是划分.

【定义 1-31】 设 A 是任意集合,π 是由 A 的若干子集组成的集合.如果下列 3 个条件成立:

(1) 对于任意 $A_i \in \pi$,均有 $A_i \neq \varnothing$;

(2) 任意 $A_i, A_j \in \pi, i \neq j$,有 $A_i \cap A_j = \varnothing$;

(3) $\bigcup_{A_i \in \pi} A_i = A$.

则称 π 是集合 A 的一种**划分**(partition).

由集合 A 的划分 π 的定义知,π 是由 A 的非空子集组成的集合,其中任意两个不同子集是不相交的,而所有这样的子集的并就是集合 A,参见图 1-13.

需要说明的是,定义 1-31 中的集合 A 被称为论域,一般情况下 A 是非空集合.为了以后讨论的方便,若 A 是空集合,则约定 A 的划分不存在,即 A 的划分为空.

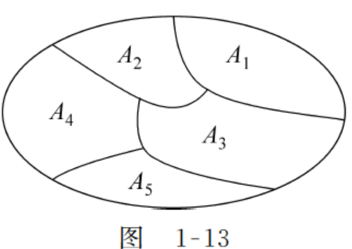


图 1-13

集合 A 的划分 π 中的每个元素称为划分的一个**块**(block 或 cell).

【例 1-53】 设 $A=\{a,b,c\}$,容易验证 $\{\{a,b\},\{c\}\}$ 是集合 A 的划分.实际上,集合 A 的所有不同的划分分别为

$$\pi_1=\{\{a,b,c\}\}, \quad \pi_2=\{\{a,b\},\{c\}\}, \quad \pi_3=\{\{a,c\},\{b\}\},$$
$$\pi_4=\{\{c,b\},\{a\}\}, \quad \pi_5=\{\{a\},\{b\},\{c\}\}$$

【例 1-54】 设 $A=\{a,b,c,d\}$,求出集合 A 的所有不同的划分(作为练习).

【例 1-55】 设 $A=\{a,b,c,d,e,f,g,h\}$,考虑下列 A 的子集合:

$$A_1=\{a,b,c,d,e\}, \quad A_2=\{d,e,f,g,h\}, \quad A_3=\{a,d,e\},$$
$$A_4=\{b,c,f\}, \quad A_5=\{g,h\}$$

则 $\{A_1,A_2\}$ 不是 A 的划分,因为 $e \in A_1 \cap A_2 \neq \varnothing$;$\{A_3,A_4\}$ 不是 A 的划分,因为 $g \notin A_3 \cup A_4$;$\{A_3,A_4,A_5\}$ 是 A 的划分.

【例 1-56】 对于整数集合 $\mathbf{Z}$,令 A_1 是所有偶数组成的集合,A_2 是所有奇数组成的集合,则 $\{A_1,A_2\}$ 是 $\mathbf{Z}$ 的划分.

【定理 1-25】 设集合 A 有两种划分 $\pi_1=\{A_i \mid i \in I\}$ 和 $\pi_2=\{B_j \mid j \in J\}$,令所有满足 $A_i \cap B_j \neq \varnothing (i \in I, j \in J)$ 的 $A_i \cap B_j$ 组成的集合为 π:

$$\pi=\{A_i \cap B_j \mid A_i \cap B_j \neq \varnothing, i \in I, j \in J\}$$

则 π 是 A 的一种划分,该划分称为划分 π_1 和 π_2 的**交叉划分**.

证 显然,π 中元素均非空,对于 π 中两个不同元素 $A_i \cap B_j$ 和 $A_k \cap B_l$,它们的交是 $\varnothing$,而 π 中所有元素的并必等于

$$\bigcup_{i \in I, j \in J}(A_i \cap B_j)=\left(\bigcup_{i \in I} A_i\right) \cap \left(\bigcup_{j \in J} B_j\right)=A \cap A=A$$

所以,π 是 A 的一种划分.

还可以定义更多个划分的交叉划分，它是**粗糙集**(rough set)理论研究中最基本的内容，它与下章介绍的等价关系密切相关. 粗糙集理论是信息科学中基于不完整数据、不精确知识的表达、学习、归纳等一种新的数学工具，参见文献[7, 10].

【例 1-57】 设集合 A 有两种划分 $\pi_1=\{A_i \mid i\in I\}$ 和 $\pi_2=\{B_j \mid j\in J\}$，问 $\pi_1\cap\pi_2$ 是否必是 A 的划分，为什么？

解 $\pi_1\cap\pi_2$ 不必是 A 的划分. 例如，取 $A=\{a,b,c,d\}$，$\pi_1=\{\{a,b\},\{c\},\{d\}\}$，$\pi_2=\{\{a,b\},\{c,d\}\}$，显然 π_1 和 π_2 是集合 A 的划分，而 $\pi_1\cap\pi_2=\{\{a,b\}\}$不是集合 A 的划分.

给定集合 A 的两种划分 $\pi_1=\{A_i \mid i\in I\}$和 $\pi_2=\{B_j \mid j\in J\}$，若对于任意 $A_i\in\pi_1$，均存在 $B_j\in\pi_2$，使得 $A_i\subseteq B_j$ 成立，则称划分 π_1 是 π_2 的**加细划分**.

显然，由定理 1-25 知 π_1 和 π_2 的交叉划分分别是 π_1 和 π_2 的加细划分. 要获得一个划分的加细，只要把划分的块划分成更小的一些块即可. 例如，学院学生分成年级学生，年级学生又可分成若干班，后者就是前者的加细.

最后介绍一个有限集合的所有划分个数问题，希望大家有所了解.

由例 1-53 知，若$|A|=3$，则 A 的所有不同的划分个数为 5. 事实上，若$|A|=4$，则 A 的所有不同的划分个数为 15.

设$|A|=n\geqslant 1$，下面考虑 A 的所有不同的划分个数 $N(n)$.

令 $S(n,k)$表示将 n 个元素集合划分成 k 个块的方案数，称 $S(n,k)$为**第二类 Stirling 数**，显然

$$N(n)=\sum_{k=1}^{n}S(n,k)$$

且有下列等式成立(其证明作为练习)：

(1) $S(n,1)=1$；

(2) $S(n,n)=1$；

(3) $S(n,2)=2^{n-1}-1$.

下面先给出一个关于 $S(n,k)$的递推关系.

【定理 1-26】 对于 $n>1$，下列关于 $S(n,k)$的递推关系成立：

$$S(n,k)=S(n-1,k-1)+kS(n-1,k)$$

证 设 $A=\{x_1,x_2,\cdots,x_n\}$，取出 A 中的一个元素 x_1，将 A 划分成 k 个块分两种情况讨论：

(1) x_1 独在一个块中，其方案数为 $S(n-1,k-1)$；

(2) x_1 不独在一个块中，这相当于将剩下的 $n-1$ 个元素划分成 k 个块，有 $S(n-1,k)$ 种方案数，再将 x_1 放在其中一个块中，有 k 种方式. 因此，此种情况的划分方案数为 $kS(n-1,k)$.

根据加法原理，有 $S(n,k)=S(n-1,k-1)+kS(n-1,k)$.

由定理 1-26 中的递推关系可得 $N(1)=1$，$N(2)=2$，$N(3)=5$，$N(4)=15$，$N(5)=52$.

1.5.2 集合的覆盖

集合的覆盖推广了集合划分的概念，其定义如下.

【定义 1-32】 设 A 是集合，如果这些非空子集的并集等于 A，则由 A 的若干非空子集

构成的集合称为 A 的**覆盖**(covering).

集合 A 的覆盖不必要求两个不同的子集不相交. 所以,集合 A 的划分是集合 A 的覆盖,但反过来不成立.

【例 1-58】 设 $A=\{a,b,c\}$,则 $\{\{a,b\},\{b,c\}\}$ 是 A 的覆盖,但不是 A 的划分.

你能写出集合 $A=\{a,b,c\}$ 的所有不同的覆盖吗? 若 $|A|=n$,则 A 的所有不同的覆盖数目是多少? 参见参考文献[6].

习　题　1.5

1. 设 $A=\{a,b,c,d\}$,求出集合 A 的所有不同的划分.

2. 对于整数集合 $\mathbf{Z}$,令

$$A_1=\{3k\mid k\in\mathbf{Z}\},\quad A_2=\{3k+1\mid k\in\mathbf{Z}\},\quad A_3=\{3k+2\mid k\in\mathbf{Z}\}$$

则 $\{A_1,A_2,A_3\}$ 是 $\mathbf{Z}$ 的划分. 试证明之.

3. 设 $\pi=\{A_i\mid i\in I\}$ 是集合 A 的一种划分,对于集合 B,所有 $A_i\cap B\neq\varnothing$ 的 $A_i\cap B$ 组成的集合是 $A\cap B$ 的划分. 试证明之.

4. 设集合 A 有两种划分 $\pi_1=\{A_i\mid i\in I\}$ 和 $\pi_2=\{B_j\mid j\in J\}$,问 $\pi_1\cup\pi_2$ 是否必是 A 的划分,为什么? $\pi_1-\pi_2$ 呢?

5. 证明:设 $n\geqslant1$,则

(1) $S(n,1)=1$;

(2) $S(n,n)=1$;

(3) $S(n,2)=2^{n-1}-1$.

6. 设 $A=\{a,b,c,d,e,f,g,h,i,j\}$,$A_1=\{a,b,c,d\}$,$A_2=\{e,f,g\}$,$A_3=\{d,e,g,i\}$,$A_4=\{d,h,j\}$,$A_5=\{h,i,j\}$,$A_6=\{a,b,c,f,h,j\}$,分别判定下列集合是否是 A 的划分、覆盖:

(1) $\{A_1,A_2,A_5\}$;

(2) $\{A_1,A_3,A_5\}$;

(3) $\{A_3,A_6\}$;

(4) $\{A_2,A_3,A_4\}$.

7. 写出集合 $A=\{a,b\}$ 的所有不同的覆盖.

1.6　集合的对等

下面讨论集合的对等,它是集合间的另一种关系. 通过集合对等以及相关内容的学习,加深对函数概念的理解,提高正确使用函数工具作为研究手段的能力.

1.6.1　集合对等的定义

【定义 1-33】 设 A,B 是集合,若存在一个 A 到 B 的双射,则称集合 A 和 B **对等**,记为 $A\sim B$.

【例 1-59】 自然数集合 $\mathbf{N}$ 与其中的所有偶数组成的集合 E 对等,试证明.

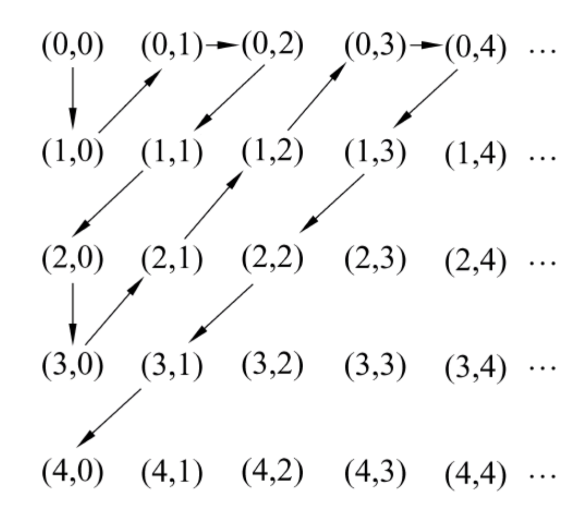
证 令 $f:\mathbf{N}\to E, f(x)=2x$，则 f 是 $\mathbf{N}$ 到 E 的双射，所以 $\mathbf{N}\sim E$.

【例 1-60】 试证明：$(0,1)\sim\mathbf{R}$.

证 令 $f:(0,1)\to\mathbf{R}, f(x)=\tan(x-1/2)\pi$. 显然 f 是双射.

【例 1-61】 试证明：$\mathbf{N}\sim\mathbf{N}\times\mathbf{N}$.

证 可按如下箭头方向建立一个 $\mathbf{N}$ 与 $\mathbf{N}\times\mathbf{N}$ 的一一对应：



【定理 1-27】 集合对等关系是等价关系(等价关系见第 2.5 节)：

(1) $A\sim A$；

(2) 若 $A\sim B$，则 $B\sim A$；

(3) 若 $A\sim B$ 且 $B\sim C$，则 $A\sim C$.

证 (1) A 上的恒等映射是 A 到 A 的双射.

(2) 因为 $A\sim B$，于是存在 A 到 B 的双射 f. 显然，f^{-1} 是 B 到 A 的双射，所以，$B\sim A$.

(3) 由已知，存在 A 到 B 的双射 f，B 到 C 的双射 g，显然，$f\circ g$ 是 A 到 C 的双射，故 $A\sim C$.

思考 关于对等关系的等价类是什么？

1.6.2 无限集合

有了集合对等的概念，就可以给出无限集合及有限集合的严格定义. 无限集合在很多问题的深入讨论中会用到.

【定义 1-34】 设 A 是集合，若 A 存在一个子集与自然数集合对等，则称 A 为**无限集合**(infinite set)，否则称 A 为**有限集合**(finite set).

【例 1-62】 自然数集合本身是无限集合.

【例 1-63】 $[0,1]$ 是无限集合，试证明.

证 显然，$\{0,1,1/2,1/3,\cdots,1/n,\cdots\}\subseteq[0,1]$. 而 $\{0,1,1/2,1/3,\cdots,1/n,\cdots\}\sim\mathbf{N}$，因此，$[0,1]$ 是无限集合.

1.6.3 集合的基数

在第 1.1 节中已经定义了有限集合的基数：有限集合 A 的基数就是 A 的元素个数，因为 $0=\varnothing, 1=\{\varnothing\}, n+1=n\cup\{n\}$. 借助于集合对等概念，可以将其扩展到无限集合.

【定义 1-35】 若集合 A 和 B 对等，则称这两个集合的**基数**(cardinality)相同.

集合 A 的基数用 $|A|$ 表示. 上述定义并未给出集合基数的定义，它只是说明了对等的两个集合 A,B 有相同的基数. 直观上理解，两个集合有相同的基数，是指这两个集合有相同的元素个数，因为它们之间可以建立一一对应，在讨论 n 个元素的 r-可重组合的计算公式时还会用到此技巧. 对于有限集合，这更容易理解. 实际上，在没有出现数的概念之前，比较两个有限集合元素个数相等就是采用对等的方法. 由于对等的集合有相同的基数，若假定自然数集合 $\mathbf{N}$ 的基数为 $\aleph_0$(阿列夫 0)：

$$|\mathbf{N}| = \aleph_0$$

则与 $\mathbf{N}$ 对等的集合的基数都是 $\aleph_0$；若假定实数集合 $\mathbf{R}$ 的基数为 $\aleph$(阿列夫)：

$$|\mathbf{R}| = \aleph$$

则与 $\mathbf{R}$ 对等的集合的基数都是 $\aleph$.

由例 1-59 知，自然数集合 $\mathbf{N}$ 与其中的全体偶数组成的集合 $\mathbf{E}$ 有相同的基数. 由例 1-60 知，$(0,1)$ 与 $\mathbf{R}$ 有相同的基数. 由例 1-61 知，$\mathbf{N}$ 与 $\mathbf{Q}$ 有相同的基数. 这些结论从直观上理解是困难的，当时的集合论创始人 G. Cantor 被这些问题所折磨而难以自拔，必须借助于映射加以理解，基数之间的运算更是这样.

在更深入的问题讨论中，还会用到可列集合和不可列集合的概念. 在学习概率统计时会用到可列集合.

1.6.4 可数集合

借助于集合对等可以定义可数集合. 设集合 $A \sim \mathbf{N}$，则存在双射 $f: A \to \mathbf{N}$，这时 $A = \{f^{-1}(0), f^{-1}(1), f^{-1}(2), \cdots\}$. 于是与自然数对等的集合有一个特点：其元素可以按第 1 个元素、第 2 个元素、第 3 个元素……一个接一个地“数”(或“列”)出来.

【定义 1-36】 能与自然数集合 $\mathbf{N}$ 对等的集合称为**可数集**(countable set)，又可称为**可列集**.

根据无限集合的定义知：**任意无限集合均存在一个可数的子集合**. 根据这一点，可以证明无限集合的特征性质：

【定理 1-28】 设 A 是无限集合，则存在 A 的一个真子集 B，使得 $A \sim B$.

证 因为 A 是无限集合，A 存在一个可数的子集 $\{a_0, a_1, a_2, \cdots\}$. 令 $B = A - \{a_0\}$，显然 B 是 A 的真子集. 建立一个 A 到 B 的双射 f 如下：任意 $x \in A$，

$$f(x) = \begin{cases} x, & x \notin \{a_0, a_1, a_2, \cdots\} \\ a_{i+1}, & x = a_i (i = 0,1,2,\cdots) \end{cases}$$

容易知道，f 是 A 到 B 的双射，故 $A \sim B$.

利用这些结论以及例 1-61 可以证明，可数集合的无限子集是可数集合；若干个可数集合的并是可数集合.

【例 1-64】 有理数集合 $\mathbf{Q}$ 是可数集合.

证 (作为练习).

由于命题变元有可数多个，容易知道命题公式组成的集合是可数集合.

1.6.5 不可数集合

是否所有无限集合都是可列的？答案是否定的.

【例 1-65】 证明：(0,1)是不可数集合.

证(采用反证法,利用对角线法则技巧) 假定(0,1)是可数集合,则$(0,1)=\{a_0,a_1,a_2,\cdots\}$. 因为$a_i\in(0,1)$,$i=0,1,2,\cdots$,将其写成唯一的无限小数形式(比如约定不允许从小数点某位开始都是0,例如0.12写成0.119999…)：

$$a_i = 0.a_{i0}a_{i1}a_{i2}a_{i3}\cdots a_{in}\cdots,\quad i=0,1,2,\cdots$$

取$r=0.b_0b_1b_2b_3\cdots b_n\cdots$,其中

$$b_n=\begin{cases}1, & a_{nn}\neq 1\\ 3, & a_{nn}=1\end{cases},\quad n=0,1,2,3,\cdots$$

这时,一方面有$r\in(0,1)$,另一方面$r\neq a_i$,$i=0,1,2,\cdots$. 这显然是一个矛盾.

由上述证明过程可知,除有限集合外,只有可数集合才能使用列举法表示该集合.

因为$(0,1)\sim\mathbf{R}$,所以实数集合是不可数集合. 由此可见,自然数集合与实数集合之间是不存在双射的,因此$\mathbf{N}$与$\mathbf{R}$不对等,进而有$\aleph_0\neq\aleph$.

注意 反证法是常用的一种证明方法. 在本章已经看到,证明方法有直接证法、举反例法、数学归纳法等. 今后还会学习一种“形式证明方法”.

1.6.6 基数的比较

最后讲解集合基数的比较.

【定义 1-37】 给定集合A,B,若存在A到B的单射,则称A的基数小于等于B的基数,记为$|A|\leqslant|B|$. 若进一步,不存在A到B的双射,则称A的基数小于B的基数,记为$|A|<|B|$.

由定义易知,若存在A到B的满射,则$|B|\leqslant|A|$.

显然,根据前面的讨论知$\aleph_0<\aleph$,即$|\mathbf{N}|<|\mathbf{R}|$. 下面的问题在使用选择公理的公理系统中不可判定[4,8]：

问题 是否存在一个集合A,满足$\aleph_0<|A|<\aleph$?

下面的定理从直观上理解很容易,但证明较困难,限于篇幅不予证明.

【定理 1-29】 对于集合A,B,若$|A|\leqslant|B|$且$|B|\leqslant|A|$,则$|A|=|B|$.

【例 1-66】 证明：$|(0,1)|=|[0,1]|$.

证 令$f:(0,1)\to[0,1]$,$f(x)=x$,f是单射,所以有$|(0,1)|\leqslant|[0,1]|$.

令$g:[0,1]\to(0,1)$,$g(x)=\dfrac{x}{3}+\dfrac{1}{6}$,$g$是单射,所以有$|[0,1]|\leqslant|(0,1)|$. 由定理1-29知,$|(0,1)|=|[0,1]|$.

习 题 1.6

1. 证明：任意无限集合均存在可数子集.
2. 证明：$(0,1)\sim[0,1]$.
3. 证明：$[0,1]\sim[a,b]$,$a<b$.
4. 有理数集合$\mathbf{Q}$是可数集合.
5. 证明：全体无理数组成的集合$\mathbf{R}-\mathbf{Q}$与$\mathbf{R}$有相同的基数.
6. 对于任意集合A,$P(A)$是A的幂集,证明：$|A|<|P(A)|$.

本章小结

1. 集合的有关概念

集合就是一些对象构成的整体. 若 x 是集合 A 中元素, 记为 $x\in A$, 否则 $x\notin A$. 理解集合就是要把集合中的元素搞清楚, 需要知道一些背景知识, 如整数、整除、偶数、素数、因数、空集、n 元组等. 表示集合可以用列举法、描述法和递归法. 集合中的元素可以是任意对象,如元素本身又可以是集合; 集合中的元素本身没有顺序关系; 集合中的元素原则上不重复.

给定集合 B, B 的子集 A 就是集合 B 中的一些元素构成的"新"集合, 记为 $A\subseteq B$. 要注意$\in$和$\subseteq$的区别. 证明两个集合相等常用到"$A=B$ 的充要条件是 $A\subseteq B$ 且 $B\subseteq A$"结论.

集合 X 的幂集 $P(X)$是 X 的所有子集构成的集合. 注意$\varnothing\in P(X)$, 要求会计算给定集合的幂集. 重要结论是: 若$|X|=n$, 则$|P(X)|=2^n$.

选取的 n 个元素 $x_1, x_2, \cdots, x_n$ 按一定顺序排列起来就是一个 n 元组$(x_1, x_2, \cdots x_n)$.

笛卡儿积 $A_1\times A_2\times\cdots\times A_n=\{(x_1, x_2, \cdots, x_n)\mid x_i\in A_i, i=1,2,\cdots,n\}$. 能熟练计算笛卡儿积. 若$|X|=m$, $|Y|=n$, 则$|X\times Y|=mn$.

2. 映射的有关概念

映射 $f: A\to B$ 就是将集合 A 的元素唯一对应到集合 B 中元素. 要深入理解映射的含义, 包括函数符号的选取和多元函数, 区分 f 和 $f(x)$的不同, 了解天花板函数和地板函数.

映射 $f: A\to B$, 若不同的 A 中元素对应不同的 B 中元素, f 就是单射; 若函数值充满整个集合 B, f 就是满射; 既是单射又是满射即为双射.

设 $f: A\to B$,若将 f 的方向逆转能得到 B 到 A 的函数, 它就是 f 的逆函数或反函数, 记为 f^{-1}. 函数 f 有反函数的充要条件是 f 是双射.

先进行映射 $f: A\to B$,再进行映射 $g: B\to C$, 可得到 A 到C 的映射, 它就是 f 与 g 的复合映射, 记为 $f\circ g$. 要求掌握两个函数的复合运算. 一般来说,$f\circ g\neq g\circ f$,但$(f\circ g)\circ h=f\circ(g\circ h)=f\circ g\circ h$. 特别应注意函数的复合运算与单射、满射和双射之间的关系.

3. 运算的定义及性质

运算的目的就是从已知元素得出新的元素, n 元运算就是 n 元函数. 集合 A 上的 n 元封闭运算 f 是指对于任意A 中的n 个元素进行 f 运算的结果仍属于集合 A. 要求掌握封闭运算的定义, 深入理解整数集合 $\mathbf{Z}$ 上的模 m 运算, 两个不同时为 0 的两个整数的最大公因数运算 gcd 和任意两个整数的最小公倍数运算 lcm. 了解运算符号的选取、运算符号的位置和运算表.

深入理解一元运算具有对合性, 二元运算具有幂等性、交换性、结合性、幺元性、零元性、逆元性和消去性等性质, 两个二元运算具有分配性、吸收性, 一个一元运算和两个二元运算具有德·摩根性, 能对给定的运算判断其性质.

4. 集合的运算

集合常见的并、交、补、差和对称差:

$$A \cup B = \{x \mid x \in A \text{ 或 } x \in B\}$$
$$A \cap B = \{x \mid x \in A \text{ 且 } x \in B\}$$
$$\overline{A} = \{x \mid x \in U, \text{且 } x \notin A\}$$
$$A - B = \{x \mid x \in A \text{ 且 } x \notin B\} = A \cap \overline{B}$$
$$A \oplus B = (A - B) \cup (B - A) = (A \cup B) - (A \cap B)$$

要求掌握集合的运算以及与运算有关的重要结论，会利用这些结论证明新的集合等式，会根据集合相等的定义证明如“$A\cup(A\cap B)=A$”、“$\overline{A\cup B}=\overline{A}\cap\overline{B}$”和“$A-B=A\cap\overline{B}$”这样的结论. 最简单情形的容斥原理：$|A\cup B|=|A|+|B|-|A\cap B|$.

5. 集合的划分与覆盖

集合的划分就是对该集合元素进行分类. 3 个元素集合有 5 种不同划分，4 个元素集合有 15 种不同划分.

了解集合的覆盖：如果 A 的若干非空子集之并就是集合 A，就得到 A 的覆盖，不要求子集之间不相交.

6. 集合的对等

利用函数可深入讨论集合之间对等关系：若两个集合之间存在一个双射，这两个集合就是对等的.

了解无限集合：若集合 A 的某子集能与自然数集合 $\mathbf{N}$ 对等，则称 A 是无限集合.

了解基数：两个对等的集合具有相同的基数，因而 $|\mathbf{Z}|=|\mathbf{N}|$ 及 $|\mathbf{R}| = |(0,1)|$.

了解可数集合：能与自然数集合 $\mathbf{N}$ 对等的集合是可数集合，否则是不可数集合. 有理数集合 $\mathbf{Q}$ 是可数集合，$(0,1)$ 是不可数集合.

了解基数的大小比较：若存在 A 到 B 的单射，则 $|A|\leqslant|B|$. 若 $|A|\leqslant|B|$ 且不存在 A 到 B 的双射，则 $|A| < |B|$.

第2章　关　　系

世间万物都存在着联系，科学研究的主要任务是发现事物间的内在规律性. 借助于集合，可以给出刻画这种联系的数学模型——关系（relation）. 这里不以个别特殊关系为研究对象，而是关注关系的一般特性.

在信息科学中，数据与数据之间总存在着一定的关系，关系这些内容对今后学习数据结构以及数据库等很多课程都是很重要的.

本章讨论的关系内容与数理逻辑、代数结构、图论以及组合计数等都有密切联系. 从这个角度去看，离散数学内容也是不离散的.

2.1　关系的概念

2.1.1　*n* 元关系的定义

在日常生活中会遇到各种各样的关系，如一个家庭与它的电话号码之间的关系、一个人与工资之间的关系、亲属关系、师生关系、上下级关系、同事关系、电影票与位置的关系等. 在数学中也出现了很多的关系，如大于关系、小于等于关系、相等关系、平行关系、相似关系、全等关系、属于关系、包含关系等. 在信息科学中，数据与数据之间存在着多种关系. 下面再看一个例子.

【引例】 设 A 是若干学生组成的集合 $A=\{$张三，李四，王五$\}$，B 是由课程组成的集合 $B=\{$英语，C 语言，离散数学，数据结构，汇编语言$\}$，C 是学习成绩组成的集合 $C=\{$优，良，合格，不合格$\}$，用 R 表示学生与课程之间的一种选修关系，如张三选修离散数学，借助于序偶可表示为（张三，离散数学），张三选修数据结构（张三，数据结构），张三选修英语（张三，英语），李四选修数据结构（李四，数据结构），王五选修 C 语言（王五，C 语言），王五选修汇编语言（王五，汇编语言），这时 R 为集合 A 与集合 B 之间的一种 2 元关系，可以将 R 表示为：

$R=\{$（张三，离散数学），（张三，数据结构），（张三，英语），（李四，数据结构），（王五，C 语言），（王五，汇编语言）$\}\subseteq A\times B$.

当选修完毕，老师会给出成绩，假定把学生所选课程的成绩也考虑在内，如张三所修的离散数学成绩为优，借助于 3 元有序组可表示为（张三，离散数学，优），可得到一个学生、课程及成绩之间的一种关系 S，它是集合 A，B，C 之间的一种 3 元关系，可以将 S 表示为：

$S=\{$（张三，离散数学，优），（张三，数据结构，良），（张三，英语，优），（李四，数据结构，优），（王五，C 语言，合格），（王五，汇编语言，良）$\}\subseteq A\times B\times C$.

这样的例子在数据结构及数据库等课程中会经常出现. 为了数学和计算机科学研究的需要，我们将学习的关系概念是所有各种各样关系的一种数学模型，其定义在引例中已现端倪，下面给出 n 元关系的定义.

【定义 2-1】 设 $A_1, A_2, \cdots, A_n$ 是集合，把 $A_1 \times A_2 \times \cdots \times A_n$ 的任意子集 R 都称为 A_1，$A_2, \cdots, A_n$ 间的 ***n* 元关系**（n-ary relation）.

从定义可以看出，$A_1, A_2, \cdots, A_n$ 间的 n 元关系 $R \subseteq A_1 \times A_2 \times \cdots \times A_n$. 在定义中，若 R 为 $A_1, A_2, \cdots, A_n$ 间的 n 元关系且 $A_1 = A_2 = \cdots = A_n = A$，即

$$R \subseteq \overbrace{A \times A \times \cdots \times A}^{n\text{个}}$$

则通常又称 R 为 A 上的 n 元关系.

结合引例知，$R \subseteq A \times B$ 是 A 与 B 间的 2 元关系，$S \subseteq A \times B \times C$ 是 A，B 与 C 间的 3 元关系.

要深入理解关系的概念，需要清楚 n 元有序组的含义，以及集合的使用. 下面的一些内容可以进一步帮助理解.

2.1.2　2 元关系

两个集合间的关系称为 2 元关系. 深入理解 2 元关系是今后学习的基础. 由于 n（$n \geqslant 3$）元关系的讨论与 2 元关系是完全类似的，若没有特殊说明，今后所涉及的关系均为 2 元关系.

R 是 A 到 B 的关系，是指 $R \subseteq A \times B$；R 是 A 上的关系，是指 $R \subseteq A \times A$.

【例 2-1】 设 $A = \{a, b\}$，$B = \{1, 2, 3\}$，若取 $R = \{(a,3), (a,2), (b,1), (b,3)\}$，则 R 是 A，B 间的一个关系. 因为

$$A \times B = \{(a,1), (a,2), (a,3), (b,1), (b,2), (b,3)\}$$

而显然 $R \subseteq A \times B$.

需要注意的是，虽然关系中的每个元素是序偶、有顺序，但关系中元素与元素之间是没有顺序的，即例 2-1 中的 R 也可以写成如下形式：

$$R = \{(a,2), (b,1), (a,3), (b,3)\}$$

根据关系的定义知，只要 $R \subseteq A \times B$，则 R 均是 A 与 B 间的一个关系或 A 到 B 的一个关系，特别地，因为 $\varnothing \subseteq A \times B$ 且 $A \times B \subseteq A \times B$，它们是 A 到 B 的关系，分别称为 A 到 B 的**空关系**和 A 到 B 的**全关系**. 特别地，A 上的空关系和全关系分别为 $\varnothing$ 和 $A \times A$.

在例 2-1 中，由于 $|A \times B| = 6$，根据幂集的元素个数的一个计数公式，很容易知道，A，B 间的关系共有 $2^6 = 64$ 个，例中所写出的 R 仅是其中的一个. 一般有下述结论.

【定理 2-1】 若 $|A| = m$，$|B| = n$，则 A，B 间的关系共有 2^{mn} 个.

显然，若 $|A| = m$，则 A 上的关系共有 2^{m^2} 个.

设 $R \subseteq A \times B$，若 $(x, y) \in R$，则称 A 中的元素 x 与 B 中的元素 y 有关系 R，通常记为 xRy. 这时，关系符号写在中间位置，它符合人们以前总是把关系符号写在两元素之间的习惯. 有时也可记为 Rxy.

【例 2-2】 设 $A = \{2, 3\}$，$B = \{1, 2, 3, 4\}$，则 A 中元素与 B 中元素有大于关系的有：$2 > 1$，$3 > 1$，$3 > 2$，即 A，B 间的大于关系 $R = \{(2, 1), (3, 1), (3, 2)\}$，显然是唯一的. 不过，$A$ 与 B 间的关系共有 $2^{2 \cdot 4} = 2^8$ 个.

以前学习过的两元素的相等关系 $=$、两直线的平行关系 $/\!/$、两图形的全等关系 $\cong$、元素与集合的属于关系 $\in$、两集合的包含关系 $\subseteq$ 等都是将关系符号写在中间位置的. 大家可能

已经注意到了，在意义清楚的情况下，关系所涉及的集合可以省略.

关系所用符号的选取方法：首先，我们是借助于集合来定义关系的，关系是集合，于是任意集合符号可以作为关系符号；其次，对于常见的很有用的关系可以给出一个固定的特殊符号，像前面提到的一些关系符号一样；当然自己还可以选一些符号表示特定的关系.

通常谈到的大于关系"$>$"是实数集合 $\mathbf{R}$ 上的大于关系，按集合记号应写成

$$>=\{(x,y) \mid x,y\in\mathbf{R}\text{ 且 }x>y\}$$

下面介绍整数集合 $\mathbf{Z}$ 上的两个重要关系：整除关系和模 m 同余关系，其大部分结论的证明放在习题中.

【例 2-3】 第 1 章已谈到，对于任意整数 m 和 n，若存在整数 q，使得 $n=qm$，称 m 整除 n，记为 $m|n$，即"$|$"是整数集合 $\mathbf{Z}$ 上的一种关系，称为 $\mathbf{Z}$ 上的整除关系.

这时 $|=\{(x,y)|x,y\in\mathbf{Z}\text{ 且 }x|y\}$. 特别地，$(2,6)$，$(-2,6)$，$(2,-6)$，$(-2,-6)$，$(2,-2)$，$(-2,2)\in|$.

显然，对于任意 $x\in\mathbf{Z}$，有 $x|x$. 整除关系还具有如下性质：对于任意整数 x,y,z,m 和 n，

(1) 若 $x|y$ 且 $y|x$，则 $x=y$ 或 $x=-y$；

(2) 若 $x|y$ 且 $y|z$，则 $x|z$；

(3) 若 $x|y$ 且 $x|z$，则 $x|(my+nz)$.

下面再介绍由伟大的数学家 K. F. Gauss 在 18 世纪末给出的整数集 $\mathbf{Z}$ 上的模 m 同余关系"$\equiv_m$"，其中 m 是正整数，它们在计算机密码学中有重要应用.

【例 2-4】 设 m 是正整数，定义整数集 $\mathbf{Z}$ 上的模 m 同余关系 $\equiv_m$ 如下：

$$(x,y)\in\equiv_m \text{ 当且仅当 } m|(x-y)$$

显然，$\equiv_m$ 是 $\mathbf{Z}$ 上的关系. 之所以称 $\equiv_m$ 为模 m 同余关系是因为 $m|(x-y)$ 当且仅当 x 除以 m 的余数等于 y 除以 m 的余数，也就是说 $x\equiv_m y$ 当且仅当 $x(\bmod m)=y(\bmod m)$，由此可以看出"模 m 同余关系"与"模 m 运算"的区别和联系.

注意 $x\equiv_m y$ 在数论中常记为 $x\equiv y(\bmod m)$，实际上是 $x(\bmod m)=y(\bmod m)$，但不要与 $x=y(\bmod m)$ 混淆.

关于模 m 同余关系有以下性质.

(1) 对任意 $x\in\mathbf{Z}$，有 $x\equiv x(\bmod m)$；

(2) 对任意 x，$y\in\mathbf{Z}$，若 $x\equiv y(\bmod m)$，则 $y\equiv x(\bmod m)$；

(3) 对任意 x，y，$z\in\mathbf{Z}$，若 $x\equiv y(\bmod m)$ 且 $y\equiv z(\bmod m)$，则 $x\equiv z(\bmod m)$；

(4) 对任意 x，$y\in\mathbf{Z}$，若 $a\equiv b(\bmod m)$ 且 $c\equiv d(\bmod m)$，则 $ax+cy\equiv bx+dy(\bmod m)$；

(5) 若 $a\equiv b(\bmod m)$ 且 $c\equiv d(\bmod m)$，则 $ac\equiv bd(\bmod m)$；

(6) 若 $a\equiv b(\bmod m)$，则 $a^n\equiv b^n(\bmod m)$，其中 n 为正整数；

(7) 若 $a\equiv b(\bmod m)$，则 $f(a)\equiv f(b)\ (\bmod m)$，其中 $f(x)$ 为整系数多项式.

关于模 m 同余关系有以下三个重要定理.

威尔逊定理(Wilson theorem) p 为素数的充要条件是 $(p-1)!\equiv-1(\bmod p)$.

欧拉定理(Euler theorem) 若整数 a 与正整数 n 互素，即 $\gcd(a, n)=1$，则 $a^{\varphi(n)}\equiv 1(\bmod n)$，其中 $\varphi(n)$ 欧拉函数.

由此可以得到：

费马小定理(Fermat little theorem). 设 p 为素数且整数 a 与 p 互素,即 $\gcd(a, p)=1$,则 $a^{p-1}\equiv 1 \pmod p$.

说明

(1) **费马大定理**(Fermat great theorem) 对任意正整数 a,b,c 和 n,当 $n>2$ 时,有 $a^n+b^n\neq c^n$(1995 年被英国数学家 Andrew Wiles 证明).

(2) 威尔逊定理从理论上给出了素数测试方法,但很不实用. 费马小定理是经常可以首先选择使用的,但由于其逆不成立,也就是说存在合数 n,即使 a 与 n 互素,$a^{n-1}\equiv 1 \pmod n$仍成立,例如 $341=11\times 31$,而 $2^{341-1}\equiv 1 \pmod{341}$,但这样的 n(称为 Carmichael 数)非常少.

与模同余关系密切相关的一个重要内容是同余方程,特别是线性同余方程. 对于给定的整数 a、b 和正整数 m,关于 x 的同余式

$$ax\equiv b \pmod m$$

称为**线性同余方程**(linear modular equation),它是一个关于模同余关系"$\equiv_m$"的式子.

显然,若 x 是 $ax\equiv b \pmod m$的解,则对于任意与 x 模 m 同余的整数 x_0 都是 $ax\equiv b \pmod m$解.

下面证明,**线性同余方程 $ax\equiv b \pmod m$ 有解的充要条件是 $\gcd(a, m)\mid b$.** 一方面,若 $ax\equiv b \pmod m$有解,则存在 $y\in \mathbf{Z}$,使得 $ax-b=my$,即 $ax-my=b$,于是 $\gcd(a, m)\mid b$. 另一方面,设 $\gcd(a, m)=d$,则存在 $x_1, y_1\in \mathbf{Z}$,使得 $ax_1+my_1=d$. 因为 $\gcd(a, m)\mid b$,存在 $c\in \mathbf{Z}$,使得 $b=dc$,于是 $a(cx_1)+m(cy_1)=b$. 令 $x=cx_1$, $y=cy_1$,因此 $ax+my=b$,由此可得 $ax\equiv b \pmod m$. 故 $ax\equiv b \pmod m$有解.

由于 $\gcd(6, 514)=2\nmid 15$, 所以 $6x\equiv 15 \pmod{514}$没有解. 若 a 与 m 互素,即 $\gcd(a, m)=1$,显然有 $\gcd(a, m)\mid b$,这时 $ax\equiv b \pmod m$有解.

从上述证明过程可知 $ax\equiv b \pmod m$的求解方法,关键是利用欧几里得算法得出使 $ax_1+my_1=d$ 成立的 $x_1, y_1\in \mathbf{Z}$. 当 m 较小时,可以用 $\mathbf{Z}_m=\{0, 1, 2, \cdots, m-1\}$中的数去"试". 例如,对于线性同余方程 $8x\equiv 4 \pmod 6$,$\mathbf{Z}_6=\{0, 1, 2, 3, 4, 5\}$中的 2 和 5 是其解,于是与 2 或 5 模 6 同余的 $x\in \mathbf{Z}$ 都是其解,即 $8x\equiv 4 \pmod 6$的全部解 x 为 $x\equiv 2 \pmod 6$和 $x\equiv 5 \pmod 6$.

公元 5—6 世纪,我国南北朝时期的一本数学著作里面有一个"物不知数"问题:"今有物,不知其数,三三数之剩二,五五数之剩三,七七数之剩二,问物几何?"这就是要求解线性同余方程组

$$\begin{cases} x\equiv 2 \pmod 3 \\ x\equiv 3 \pmod 5 \\ x\equiv 2 \pmod 7 \end{cases}$$

中国剩余定理(Chinese remainder theorem) 设正整数 $m_1, m_2, \cdots, m_k$ 两两互素,则线性同余方程组

$$\begin{cases} x\equiv a_1 \pmod{m_1} \\ x\equiv a_2 \pmod{m_2} \\ \quad\vdots \\ x\equiv a_k \pmod{m_k} \end{cases}$$

有整数解，且在模 $m=m_1m_2\cdots m_k$ 下解是唯一的，即任意两个解都是模 m 同余的.

记 $M_i=\frac{m}{m_i}, i=1,2,\cdots,k$. 由于 $\gcd(M_i,m_i)=1$，存在整数 x_i 使得 $M_ix_i\equiv1 \pmod{m_i}$，$i=1,2,\cdots,k$. 取

$$x=a_1M_1x_1+a_2M_2x_2+\cdots+a_kM_kx_k$$

即满足上述线性同余方程组.

在“物不知数”问题中，$m=3\cdot5\cdot7=105, M_1=35, M_2=21, M_3=15$. 而 $35\cdot2\equiv1 \pmod 3$，$21\cdot1\equiv1 \pmod 5$，$15\cdot1\equiv1 \pmod 7$，于是 $x_1=2, x_2=1, x_3=1$，所以 $x=2\cdot35\cdot2+3\cdot21\cdot1+2\cdot15\cdot1=233$. 在模 $m=105$ 下解是 23，这是最小解. 请注意还有其他解.

1978 年发布的 RSA(Rivest-Shamir-Adleeman)公钥密码的基础是 Euler 定理，其安全性依赖于大数的因数分解的困难性，该方法综合利用了素数、Euler 函数、模运算、互素、线性同余方程等，有关内容，参见文献[23].

对于 A 上的关系，有一个特别重要的关系：A 上的恒等关系 I_A，其定义如下.

【定义 2-2】 设 A 是集合，称 $I_A=\{(x,x)\mid x\in A\}$ 为 A 上的**恒等关系**.

【例 2-5】 设 $A=\{a,b,c,d\}$，则 $I_A=\{(a,a),(b,b),(c,c),(d,d)\}$ 是 A 上的恒等关系.

注意 $\{(a,a),(b,b),(c,c)\}$ 不是 $A=\{a,b,c,d\}$ 上的恒等关系.

由前面的讨论知，通常一个集合到一个集合的关系非常多，但在一个实际问题中，需要找到一个与问题有关的有助于问题解决的关系，这就要求逐渐学会自己定义关系. 仔细体会下面的几个关系的定义.

【例 2-6】 设 R 是复数集合 $\mathbf{C}$ 上的关系，定义如下：

$$xRy \text{ 当且仅当 } x-y=a+b\mathrm{i}$$

其中 a，b 为非负整数.

【例 2-7】 设 R 是非零复数集合 $\mathbf{C}^*=\mathbf{C}-\{0\}$ 上的关系，定义如下：

$$(x+y\mathrm{i})R(u+v\mathrm{i}) \text{ 当且仅当 } xu>0$$

【例 2-8】 设 A 是正整数的序偶组成的集合 $A=\{(x,y)\mid x,y \text{ 是正整数}\}$，定义 A 上的关系 R 如下：

$$(x,y)R(u,v) \text{ 当且仅当 } xv=yu$$

【例 2-9】 设 $A=P(\{a,b,c\})$，定义 A 上的关系 R 如下：

$$R=\{(X,Y)\mid X,Y\in A, X\cap Y\neq\varnothing\}$$

2.1.3 关系的定义域和值域

【定义 2-3】 设 $R\subseteq A\times B$，R 的**定义域**(domain)是由所有 $(x,y)\in R$ 中的 x 组成的集合，即

$$\mathrm{dom}R=\{x\mid \text{存在 } y\in B, \text{使}(x,y)\in R\}$$

R 的**值域**(range)由所有 $(x,y)\in R$ 中的 y 组成的集合为

$$\mathrm{ran}R=\{y\mid \text{存在 } x\in A, \text{使}(x,y)\in R\}$$

显然，若 $R\subseteq A\times B$，则 $\mathrm{dom}R\subseteq A$，$\mathrm{ran}R\subseteq B$. 就例 2-2 来说，$\mathrm{dom}R=\{2,3\}$，$\mathrm{ran}R=\{1,2\}$.

【例 2-10】 设 $A=\{1,2,3,4\}$，R 是 A 上的关系，定义如下：

$$R=\{(x,y)\mid x,y\in A\text{ 且}(y-x)/2\text{ 是整数}\}$$

试求出 R 以及 $\mathrm{dom}R$ 和 $\mathrm{ran}R$.

解 由已知，有 $R=\{(1,1),(1,3),(2,2),(2,4),(3,1),(3,3),(4,2),(4,4)\}$，进一步得出 $\mathrm{dom}R=\{1,2,3,4\}$，$\mathrm{ran}R=\{1,2,3,4\}$.

2.1.4 关系的表示

前面介绍的是关系的集合表示. 对于有限集合 A 和 B，以及 A 到 B 的关系 R，为了更直观地理解关系 R，特别是后面要学习的关系的性质等有关内容，需要掌握关系 R 的关系图 G_R 表示. 同时，为了用代数知识处理关系以及借助于计算机处理关系，需要掌握关系 R 的关系矩阵 $\boldsymbol{M}_R$ 表示.

1. 关系图(graph of relation)

分两种情形讨论关系图的画法.

情形 1 R 是 A 到 B 的关系(包括 R 是 A 上的关系). 通常将集合中的所有元素用点(小的空心点或实点)表示，集合 A 画在左边，集合 B 画在右边；若 $(x,y)\in R$，则从集合 A 中的元素 x 到集合 B 中的元素 y 画一条有向弧(通常称为有向边). 所画出的图形就是关系 R 的关系图 G_R.

【例 2-11】 设 $A=\{a,b,c,d\}$，$B=\{1,2,3\}$，A 到 B 的关系 R 取为

$$R=\{(a,2),(a,3),(c,2),(d,2)\}$$

则关系 R 的关系图 G_R 如图 2-1 所示.

情形 2 R 是 A 上的关系. 可以按情形 1 进行处理，但通常只将集合 A 中所有的元素用点(小的空心点或实点)表示，画到一块，点与点之间没有顺序关系；若 $(x,y)\in R$，则从元素 x 到元素 y 画一条有向边. 所画出的图形就是关系 R 的关系图 G_R.

【例 2-12】 设 $A=\{a,b,c,d\}$，A 上的关系 R 取为

$$R=\{(a,b),(a,c),(c,a),(d,c),(d,d)\}$$

则关系 R 的关系图 G_R 如图 2-2 所示.

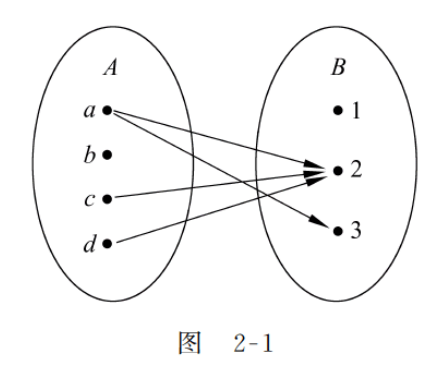


图 2-1

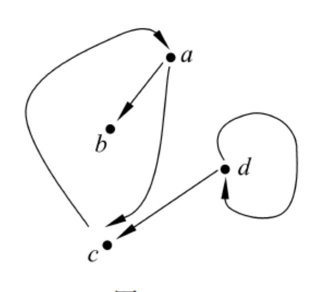


图 2-2

在画关系图时，集合 A(及集合 B)中所有元素都要用一个点表示，如图 2-1 中的元素 b 及元素 1. 只要 $(x,y)\in R$，则都要从元素 x 到元素 y 画一条有向边，这意味着，关系 R 中有多少个序偶，则在关系图 G_R 中就有多少条有向边，特别要注意的是图 2-2 中元素 d 到 d 的一条有向边，它又称为 d 到 d 的一个环(或自环).

2. 关系矩阵(matrix of relation)

在求关系矩阵时,不需要分成上述两种情形讨论. 令 $A=\{x_1,x_2,\cdots,x_m\}$, $B=\{y_1,y_2,\cdots,y_n\}$(对于 A 上的关系 R, 有 $B=A$),对于给定的 A 到 B 的关系 R, 其关系矩阵 $\boldsymbol{M}_R=(m_{ij})_{m\times n}$ 是一个 $m\times n$ 矩阵,其中

$$m_{ij}=\begin{cases}1, & (x_i,y_j)\in R\\ 0, & (x_i,y_j)\notin R\end{cases}$$

若将矩阵写成通常的表格形式,则如表 2-1 所示.

表 2-1

	y_1	y_2	$\cdots$	y_n
x_1	m_{11}	m_{12}	$\cdots$	m_{1n}
x_2	m_{21}	m_{22}	$\cdots$	m_{2n}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
x_m	m_{m1}	m_{m2}	$\cdots$	m_{mn}

【例 2-13】 写出例 2-11 所给出的关系 R 的关系矩阵 $\boldsymbol{M}_R$.

解

$$\boldsymbol{M}_R=\begin{array}{c}\\ a\\ b\\ c\\ d\end{array}\begin{array}{c}\begin{matrix}1 & 2 & 3\end{matrix}\\ \begin{bmatrix}0 & 1 & 1\\ 0 & 0 & 0\\ 0 & 1 & 0\\ 0 & 1 & 0\end{bmatrix}_{4\times 3}\end{array}$$

【例 2-14】 写出例 2-12 所给出的关系 R 的关系矩阵 $\boldsymbol{M}_R$.

解

$$\boldsymbol{M}_R=\begin{array}{c}\\ a\\ b\\ c\\ d\end{array}\begin{array}{c}\begin{matrix}a & b & c & d\end{matrix}\\ \begin{bmatrix}0 & 1 & 1 & 0\\ 0 & 0 & 0 & 0\\ 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 1\end{bmatrix}_{4\times 4}\end{array}$$

需要说明的是,任何 A 到 B 的关系 R,令 $X=A\cup B$,则 R 可看作 X 上的关系,这是因为由 $R\subseteq A\times B$,很容易可推出 $R\subseteq(A\cup B)\times(A\cup B)=X\times X$.

2.1.5 函数的关系定义

最后,借助于关系(关系是集合)可以对函数给出一个严格定义.在定义之前,先结合一个具体的函数例子,看一看是如何将函数转换为关系的.

【例 2-15】 设集合 $A=\{a,b,c\}$, $B=\{1,2,3\}$,令 $f:A\to B$,定义如下: $f(a)=2$, $f(b)=3$, $f(c)=3$. 以前是将 f 仅仅看作是一个函数符号,现在将 f 看作是一个关系符号:若 $f(x)=y$,则规定 $(x,y)\in f$. 于是,有

$$f=\{(a,2),(b,3),(c,3)\}$$

显然,若 $f:A\to B$,则 f 是集合 A 到 B 的一个关系. 但不是任何一个集合 A 到 B 的关系都可构成集合 A 到 B 的函数的,例如 $R=\{(a,2),(a,3),(c,3)\}$.

若 $f:A\to B$，则根据函数的定义知，由 f 所得到的关系满足两个条件：

(1) $\mathrm{dom}f=A$：A 中任意元素都有 B 中元素与之对应.

(2) 对于任意 $x\in A$，若 $(x,y_1)\in f$ 且 $(x,y_2)\in f$，则 $y_1=y_2$：一个 $x\in A$ 只能有唯一的 y 与之对应.

当然，反过来知道，满足上述(1)及(2)的 A 到 B 的关系是 A 到 B 的函数. 因此，借助于关系给函数下如下定义.

【定义 2-4】 设 A,B 是集合，f 是 A 到 B 的关系，若 f 满足下面两个条件：

(1) $\mathrm{dom}f=A$.

(2) 对于任意 $x\in A$，若 $(x,y_1)\in f$ 且 $(x,y_2)\in f$，则 $y_1=y_2$(单值性)，则称 f 为 A 到 B 的**函数**.

若 f 为 A 到 B 的函数，与第 1 章一样，记为 $f:A\to B$.

注意 记号 $f:A\to B$ 与 $f\subseteq A\times B$ 的区别.

函数的这种定义与第 1 章所给的定义，本质上是相同的. 前面提到，集合是现代数学中的最基本概念，意味着其他概念都可以借助于它加以定义. 同时，函数的关系定义，有效地避开了"对应"这个不容易交代清楚的概念.

显然，关系是函数的推广. 这样，以前的函数符号就是关系符号，也就是集合符号. 要求大家能转变观念，可以将第 1 章第 2 节例 1-5 写出的 8 个函数用关系表示出来；也要求大家对于给定的 A 到 B 的关系能判断出是否是 A 到 B 的函数.

【例 2-16】 判断自然数集合 **N** 上的下列关系能否构成函数.

(1) $f=\{(x,y)\mid x,y\in\mathbf{N},x+y<5\}$.

(2) $f=\{(x,y)\mid x,y\in\mathbf{N},y$ 为小于等于 x 的素数个数$\}$，p 是素数(prime)或质数是指 $p>1$ 且 p 的正的公约数只能是 1 或它本身.

解 (1) 显然，$(2,1)\in f$，$(2,2)\in f$，不满足单值性要求，所以 f 不可能构成函数.

(2) 对于任意 $x\in\mathbf{N}$，满足小于等于 x 的素数个数是唯一的，且一定属于 **N**，即与 x 对应的 y 是唯一的，根据函数的关系定义，(1)和(2)都满足，故 f 是 **N** 上的函数.

习　题　2.1

1. 试举出两个熟悉的 3 元关系的例子.

2. 设 $A=\{a,b\}$，试求出所有 A 上的关系，并验证定理 2-1 的结论.

3. 设 $A=\{0,1,2,3,4\}$，A 上的关系 $R=\{(x,y)\mid x=y+1$ 或 $y=x/2\}$，试用列举法求出 R.

4. 分别判断下列各式是否正确：$4\mid 6$，$3\mid -12$，$-3\mid 0$，$0\mid -3$，$0\mid 0$，$2\mid -2$，$-2\mid 2$.

5. 对于任意整数 x,y,z,m 和 n，证明以下结论.

(1) 若 $x\mid y$ 且 $y\mid x$，则 $x=y$ 或 $x=-y$.

(2) 若 $x\mid y$ 且 $y\mid z$，则 $x\mid z$.

(3) 若 $x\mid y$ 且 $x\mid z$，则 $x\mid(my+nz)$.

6. 如果关于 x 的整系数方程 $a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n=0$ 有为整数的根 λ，则$\lambda\mid a_n$.

7. 设 m 为正整数，证明

(1) 对于任意 $x\in\mathbf{Z}$，$x\equiv x(\mathrm{mod}\ m)$.

(2) 对于任意 $y,z\in\mathbf{Z}$,若 $x\equiv y(\text{mod } m)$,则 $y\equiv x(\text{mod } m)$.

(3) 对于任意 $x,y,z\in\mathbf{Z}$,若 $x\equiv y(\text{mod } m)$且 $y\equiv z(\text{mod } m)$,则 $x\equiv z(\text{mod } m)$.

8. 证明:若 $a\equiv b(\text{mod } m)$且 $c\equiv d(\text{mod } m)$,则

(1) 对任意 $x,y\in\mathbf{Z}$,$ax+cy\equiv bx+dy(\text{mod } m)$.

(2) $ac\equiv bd(\text{mod } m)$.

(3) 对于任意正整数 n,$a^n\equiv b^n(\text{mod } m)$.

(4) 对于任意整系数多项式 $f(x)$,$f(a)\equiv f(b)\ (\text{mod } m)$.

9. 证明威尔逊定理:p 为素数的充要条件是$(p-1)!\equiv -1(\text{mod } p)$.

10. 证明欧拉定理:若 a 与 n 互素,即 $\gcd(a, n)=1$,则 $a^{\varphi(n)}\equiv 1(\text{mod } n)$,其中 $\varphi(n)$欧拉函数.

11. 线性同余方程 $ax\equiv b(\text{mod } m)$有解的充要条件是 $\gcd(a, m)\mid b$.

12. 证明中国剩余定理:设正整数 $m_1,m_2,\cdots,m_k$ 两两互素,则线性同余方程组

$$\begin{cases} x\equiv a_1(\text{mod } m_1) \\ x\equiv a_2(\text{mod } m_2) \\ \qquad\vdots \\ x\equiv a_k(\text{mod } m_k) \end{cases}$$

有整数解,且在模 $m=m_1m_2\cdots m_k$ 下解是唯一的,即任意两个解都是模 m 同余的.

13. 对于如下给出的 4 个关系,用列举法求出所给关系 R,$\text{dom}R$,$\text{ran}R$,画出 R 的关系图 G_R,写出 R 的关系矩阵 $\mathbf{M}_R$.

(1) $A=\{0,1,2,3,4,5,6\}$,$R=\{(x,y)\mid x\geqslant 2$ 且 $x\mid y\}$.

(2) $A=\{0,1,2,3,4,5\}$,$R=\{(x,y)\mid 1\leqslant x-y\leqslant 2\}$.

(3) $A=\{2,3,4,5,6\}$,$R=\{(x, y)\mid \gcd(x, y)=1\}$.

(4) $A=\{0,1,2,3,4,5,6\}$,$R=\{(x,y)\mid x>y$ 且 y 是素数$\}$.

14. 指出图 2-3～图 2-6 的关系图所给出的关系 R 是否是 A 到 B 的函数,为什么?

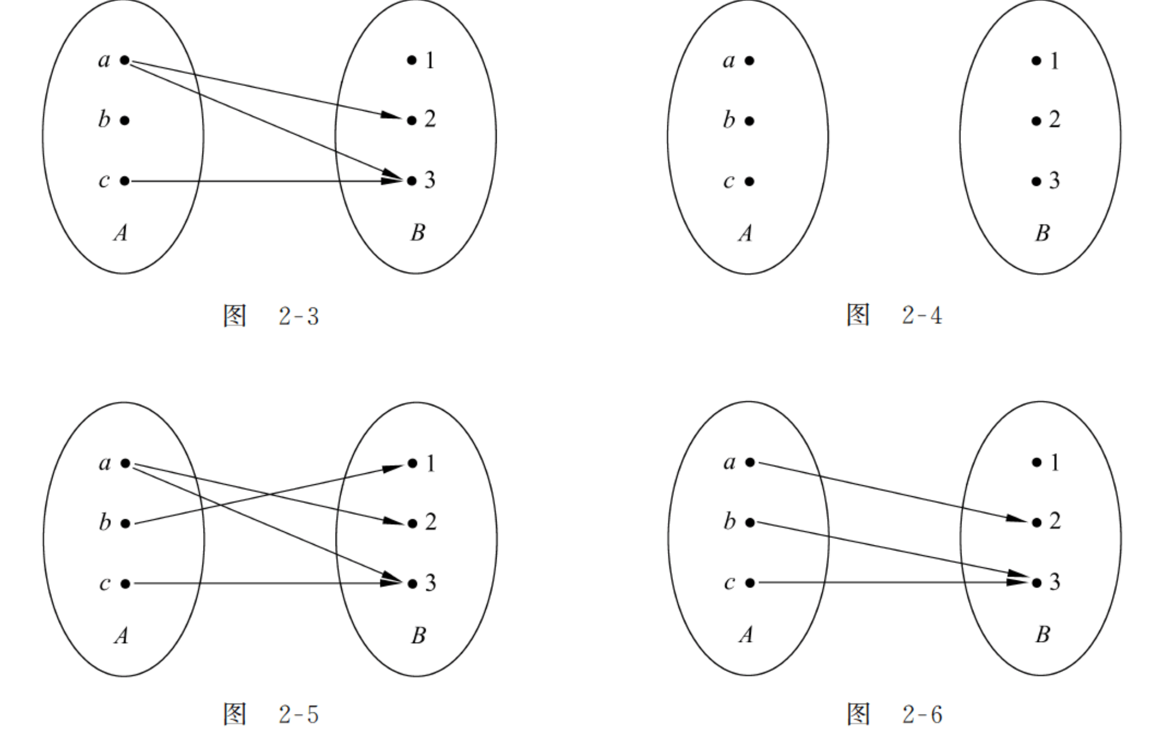


图 2-3　　图 2-4

图 2-5　　图 2-6

15. 判断实数集合 $\mathbf{R}$ 上的下列关系能否构成函数.

(1) $f=\{(x,y)\mid x,y\in\mathbf{R}, x=y^2\}$.

(2) $f=\{(x,y)\mid x,y\in\mathbf{R}, y=x^2\}$.

2.2 关系的运算

讨论关系的运算是为了从已知的关系得出新的关系.

2.2.1 关系的集合运算

根据关系的定义知,关系就是集合.所以在第 1 章中所给出的集合的五种常见运算,关系也有.

设 R 和 S 是集合 A 到 B 的关系,即 $R,S\subseteq A\times B$,则**关系的并、交、补、差及对称差(环和)**运算

$$R\cup S, R\cap S, \bar{R}, R-S, R\oplus S$$

就是相应的集合运算,其运算性质就是集合的运算性质.

显然只要 $R,S\subseteq A\times B$,就有 $R\cup S, R\cap S, \bar{R}, R-S, R\oplus S\subseteq A\times B$.特别地,若 R 和 S 是集合 A 上的关系,则其集合运算后仍为 A 上的关系.

注意 若 $R\subseteq A\times B$,因为 A 到 B 的全关系为 $A\times B$,它就是讨论集合时的全集,所以 $\bar{R}=A\times B-R$.若 $R\subseteq A\times A$,$A\times A$ 是 A 上的全关系,这时 $\bar{R}=A\times A-R$.

【例 2-17】 设 $A=\{2,3,4\}$,令 R 为 A 上的整除关系,S 为 A 上的小于关系,分别计算 $R\cup S, R\cap S, \bar{R}, R-S, R\oplus S$.

解 先求出 R 和 S:

$$R=\{(2,2),(2,4),(3,3),(4,4)\}$$
$$S=\{(2,3),(2,4),(3,4)\}$$

再计算 $R\cup S, R\cap S, \bar{R}, R-S, R\oplus S$:

$$R\cup S=\{(2,2),(2,4),(3,3),(4,4),(2,3),(3,4)\}$$
$$R\cap S=\{(2,4)\}$$
$$\bar{R}=A\times A-R=\{(2,3),(3,2),(4,2),(3,4),(4,3)\}$$
$$R-S=\{(2,2),(3,3),(4,4)\}$$
$$R\oplus S=(R-S)\cup(S-R)=\{(2,2),(3,3),(4,4)\}\cup\{(2,3),(3,4)\}$$
$$=\{(2,2),(3,3),(4,4),(2,3),(3,4)\}$$

2.2.2 关系的逆运算

若 x 与 y 有关系 R,这时 y 与 x 之间的关系就是 R 的逆关系.

【定义 2-5】 设 $R\subseteq A\times B$,R 的**逆关系**(inverse)R^{-1}定义为

$$R^{-1}=\{(y,x)\mid(x,y)\in R\}$$

显然,若 $R\subseteq A\times B$,则 R^{-1}是集合 B 到 A 的关系,即 $R^{-1}\subseteq B\times A$.在本书中,$R$ 的逆关系不用符号 R^C 表示,是考虑到逆关系 R^{-1}在一定的条件下可以构成逆函数.

很容易知道,大于关系“$>$”的逆关系就是小于关系“$<$”,即有 $>^{-1}=<$,如 $3>2$,则

$2<3$;集合包含关系"$\subseteq$"的逆关系是"$\supseteq$",即$\subseteq^{-1}=\supseteq$,如$A\subseteq B$,则$B\supseteq A$;关系"x是y的老师"的逆关系是"y是x的学生"等.再举一个例子.

【例 2-18】 设$A=\{a,b,c,d\}$,$B=\{1,2,3\}$,若$R=\{(a,3),(c,2),(a,2),(b,2)\}$,求$R^{-1}$.

解 容易知道,$R^{-1}=\{(3,a),(2,c),(2,a),(2,b)\}$.

根据给定的关系R的关系图G_R,很容易画出其逆关系R^{-1}的关系图$G_{R^{-1}}$;从关系R的关系矩阵$\boldsymbol{M}_R$,很容易求出其逆关系R^{-1}的关系矩阵$\boldsymbol{M}_{R^{-1}}$,请读者自己总结其规律.

下面讨论关系逆运算的性质.

由逆运算的定义,易知:

【定理 2-2】 $(R^{-1})^{-1}=R$.

下面的定理给出的是逆运算与关系的集合运算之间的性质.

【定理 2-3】 设$R,S\subseteq A\times B$,则下列结论成立.

(1) $(R\cup S)^{-1}=R^{-1}\cup S^{-1}$.

(2) $(R\cap S)^{-1}=R^{-1}\cap S^{-1}$.

(3) $(\bar{R})^{-1}=\overline{R^{-1}}$.

证 只证明(1),其余留作练习.

先证明$(R\cup S)^{-1}\subseteq R^{-1}\cup S^{-1}$:任意$(u,v)\in(R\cup S)^{-1}$(显然,$u\in B$,$v\in A$),可得出$(v,u)\in R\cup S$,于是$(v,u)\in R$或$(v,u)\in S$,从而$(u,v)\in R^{-1}$或$(u,v)\in S^{-1}$,因此,$(u,v)\in R^{-1}\cup S^{-1}$.

上述过程可以反过来,就可以证明$R^{-1}\cup S^{-1}\subseteq(R\cup S)^{-1}$. 结论(1)得证.

至于逆运算与关系的差及对称差(环和)运算的有关性质,可以从定理 2-3 推出.

2.2.3 关系的复合运算

1. 关系 R 与关系 S 的复合 $R\circ S$

若x与y有关系R,且y与z有关系S,这时x与z之间的关系就是关系R与S的复合.

【定义 2-6】 设A,B,C是集合,若$R\subseteq A\times B$,$S\subseteq B\times C$,则关系R与关系S的**复合**(composition)$R\circ S$定义为

$$R\circ S=\{(x,z)\mid x\in A,z\in C,\text{存在 } y\in B\text{ 使得}(x,y)\in R,(y,z)\in S\}$$

对于初学者来说,关系的这种运算是比较难理解的.先看一个例子.

【例 2-19】 设$A=\{a,b,c,d\}$,$B=\{1,2,3,4\}$,$C=\{\alpha,\beta,\gamma,\delta\}$,$A$到$B$的关系$R$取为

$$R=\{(a,1),(a,2),(b,2),(d,3),(c,4)\}$$

B到C的关系S取为

$$S=\{(1,\alpha),(2,\beta),(2,\delta),(3,\beta)\}$$

试计算$R\circ S$.

解 根据复合运算的定义,求出所有的满足条件的序偶(x,z).

(1) $(a,\alpha)\in R\circ S$,因为存在$y=1\in B$,使得$(a,1)\in R$,$(1,\alpha)\in S$.

(2) $(a,\beta)\in R\circ S$,因为存在$y=2\in B$,使得$(a,2)\in R$,$(2,\beta)\in S$.

(3) $(a,\delta)\in R\circ S$,因为存在$y=2\in B$,使得$(a,2)\in R$,$(2,\delta)\in S$.

(4) $(b,\beta)\in R\circ S$,因为存在$y=2\in B$,使得$(b,2)\in R$,$(2,\beta)\in S$.

(5) $(b,\delta)\in R\circ S$,因为存在 $y=2\in B$,使得$(b,2)\in R$,$(2,\delta)\in S$.

(6) $(d,\beta)\in R\circ S$,因为存在 $y=3\in B$,使得$(d,3)\in R$,$(3,\beta)\in S$.

于是,$R\circ S=\{(a,\alpha),(a,\beta),(a,\delta),(b,\beta),(b,\delta),(d,\beta)\}$.

借助于关系图,可以用图 2-7 来理解上面所给出的例子.

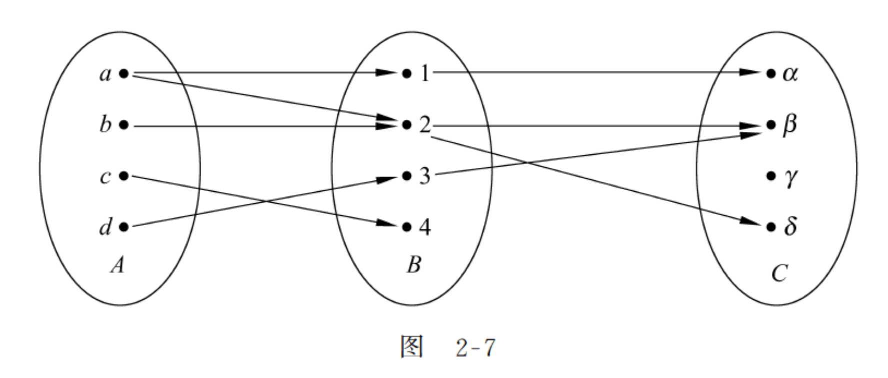


图 2-7

在这个例子中需要注意的是,虽然有$(c,4)\in R$,但不存在$(4,z)\in S$,所以,不存在$(c,z)\in R\circ S$,这是初学者要注意的问题.

由复合运算的定义可知,若 $R\subseteq A\times B$,$S\subseteq B\times C$,则 $R\circ S\subseteq A\times C$,即 $R\circ S$ 是集合 A 到 C 的关系.

也可以借助于一些例子去理解关系的复合:若 x 是 y 的母亲,y 是 z 的妻子,则 x 是 z 的岳母;若 x 是 y 的父亲,y 是 z 的父亲,则 x 是 z 的祖父.自己可以再举出一些类似的例子,以帮助我们理解两个关系的复合.

需要注意的是,不是任意两个关系都可以求复合的.根据复合运算的定义知,只有在 $R\subseteq A\times B$,$S\subseteq B\times C$ 时,有一个公共的集合 B,$R\circ S$ 才有意义.换句话说,即使 $R\circ S$ 有意义,不能保证 $S\circ R$ 有意义.就上面所举的例 2-19 来说,虽然 $R\circ S$ 有意义,但 $S\circ R$ 没有意义.

若 $R\subseteq A\times B$,$S\subseteq B\times A$,则 $R\circ S$ 及 $S\circ R$ 都有意义.特别地,若 R,S 是 A 上的关系,则 $R\circ S$ 及$S\circ R$ 都有意义.但即使 $R\circ S$ 及 $S\circ R$ 都有意义,也不能保证 $R\circ S=S\circ R$,见下面的例 2-20.也就是说,关系的复合运算不满足交换律,即一般来说,

$$R\circ S\neq S\circ R$$

【例 2-20】 设 $A=\{0,1,2,3\}$,A 上的关系 R 和 S 定义如下

$$R=\{(x,y)\mid x,y\in A,y=x+1\text{ 或 }y=x/2\}$$
$$S=\{(x,y)\mid x,y\in A,x=y+2\}$$

计算 $R\circ S$ 及 $S\circ R$.

解 由题意知,$R=\{(0,1),(1,2),(2,3),(0,0),(2,1)\}$,$S=\{(2,0),(3,1)\}$,于是有,$R\circ S=\{(1,0),(2,1)\}$,$S\circ R=\{(2,1),(2,0),(3,2)\}$.

显然有,$R\circ S\neq S\circ R$,所以,在讨论两个关系复合的时候,要注意它们的顺序.

【例 2-21】 设 $A=\{a,b,c,d\}$,A 上的关系 R、S 和 T 分别为 $R=\{(b,b),(b,c),(c,a)\}$,$S=\{(b,a),(c,a),(c,d),(d,c)\}$,$T=\{(a,b),(c,b),(d,a)\}$,试计算$(R\circ S)\circ T$ 和 $R\circ(S\circ T)$.

解

(1) 由于 $R\circ S=\{(b,a),(b,d)\}$,于是$(R\circ S)\circ T=\{(b,b),(b,a)\}$.

(2) 因为 $S\circ T=\{(b,b),(c,b),(c,a),(d,b)\}$,所以 $R\circ(S\circ T)=\{(b,b),(b,a)\}$.

下面讨论关系复合运算的性质.

前面已经知道,关系的复合运算不满足交换律,但可以证明:关系的复合运算满足结合律.

【定理 2-4】 设 $R\subseteq A\times B$,$S\subseteq B\times C$,$T\subseteq C\times D$,则下式成立

$$(R\circ S)\circ T=R\circ(S\circ T)$$

证 先证明$(R\circ S)\circ T\subseteq R\circ(S\circ T)$:任意$(x,w)\in(R\circ S)\circ T$,由复合运算的定义知,存在$z\in C$使得$(x,z)\in R\circ S$且$(z,w)\in T$. 再次根据复合运算的定义知,存在$y\in B$使得$(x,y)\in R$且$(y,z)\in S$. 因为$(y,z)\in S$且$(z,w)\in T$,所以$(y,w)\in S\circ T$. 又因为$(x,y)\in R$,于是有$(x,w)\in R\circ(S\circ T)$. 因此,有$(R\circ S)\circ T\subseteq R\circ(S\circ T)$.

类似地,可以证明:$R\circ(S\circ T)\subseteq(R\circ S)\circ T$. 实际上,上述过程可倒推回去.

所以,有$(R\circ S)\circ T=R\circ(S\circ T)$.

正因为关系的复合运算满足结合律,所以$R\circ S\circ T$有意义,可以理解成$(R\circ S)\circ T$,也可以是$R\circ(S\circ T)$.

【定理 2-5】 设 $R\subseteq A\times B$,$S,T\subseteq B\times C$,则:

(1) $R\circ(S\cup T)=(R\circ S)\cup(R\circ T)$;

(2) $R\circ(S\cap T)\subseteq(R\circ S)\cap(R\circ T)$.

证 只证明(2),(1)留作练习.

任意$(x,z)\in R\circ(S\cap T)$,根据定义知,存在$y\in B$使得$(x,y)\in R$,$(y,z)\in S\cap T$,这时$(y,z)\in S$且$(y,z)\in T$,进而由定义有$(x,z)\in R\circ S$且$(x,z)\in R\circ T$,于是有$(x,z)\in(R\circ S)\cap(R\circ T)$. 所以结论成立.

需要注意的是,一般来说,等式$R\circ(S\cap T)=(R\circ S)\cap(R\circ T)$不成立,即复合运算对关系的交运算不满足分配律. 下面是一个例子.

【例 2-22】 设 $A=\{a,b,c,d\}$,A上的关系R、S和T分别取为

$$R=\{(a,b),(a,c)\},S=\{(b,d)\},T=\{(c,d)\}$$

显然,$S\cap T=\varnothing$,进而$R\circ(S\cap T)=\varnothing$. 另一方面,$R\circ S=R\circ T=\{(a,d)\}$,所以,$(R\circ S)\cap(R\circ T)=\{(a,d)\}$,因此有$R\circ(S\cap T)\neq(R\circ S)\cap(R\circ T)$.

下述定理给出复合运算与逆运算之间的关系.

【定理 2-6】 设 $R\subseteq A\times B$,$S\subseteq B\times C$,则$(R\circ S)^{-1}=S^{-1}\circ R^{-1}$.

证 先证明$(R\circ S)^{-1}\subseteq S^{-1}\circ R^{-1}$:任意$(u,v)\in(R\circ S)^{-1}$,由逆关系的定义有$(v,u)\in R\circ S$,进而存在$y\in B$,使得$(v,y)\in R$,$(y,u)\in S$. 于是,$(y,v)\in R^{-1}$,$(u,y)\in S^{-1}$,根据复合运算的定义有$(u,v)\in S^{-1}\circ R^{-1}$.

再证明$S^{-1}\circ R^{-1}\subseteq(R\circ S)^{-1}$:上述过程逆推即证. 定理得证.

下述定理给出复合运算与恒等关系之间的一个结论.

【定理 2-7】 设 $R\subseteq A\times B$,则:

(1) $I_A\circ R=R$;

(2) $R\circ I_B=R$.

证 (留作练习).

2. 关系 R 的方幂运算 R^n

设$R\subseteq A\times B$,由复合运算的定义知,一般来说$R\circ R$都没有意义,除非R是集合A上的关系. 为了讨论关系R的**方幂运算**(power of relation),需要假定$R\subseteq A\times A$.

【定义 2-7】 设 $R\subseteq A\times A$,定义 $R^0=I_A$(A 上的恒等关系),$R^1=R$, $R^n=\overbrace{R\circ R\circ\cdots\circ R}^{n个}$,$n\geqslant 2$.

由于关系的复合运算满足结合律,上述定义是有意义的. 需要注意的是,关系 R 是集合,n 个集合可以定义笛卡儿积运算,参见第 1 章有关内容,但这里的 R^n 是 n 个 R 求复合运算, 这根据上下文不难判别. 在很多时候,R^2 写成 $R\circ R$.

显然,对于非负整数 m,n,下面的结论成立.

【定理 2-8】 设 $R\subseteq A\times A$,对于非负整数 m,n,有:

(1) $R^m\circ R^n=R^{m+n}$;

(2) $(R^m)^n=R^{mn}$;

(3) $(R^m)^{-1}=(R^{-1})^m$.

【例 2-23】 设 $A=\{a,b,c\}$,集合 A 上的关系 $R=\{(a,b),(b,c),(c,a)\}$,试计算 R^n(n 为正整数).

解 $R^1=R=\{(a,b),(b,c),(c,a)\}$,

$R^2=\{(a,c),(b,a),(c,b)\}$,

$R^3=\{(a,a),(b,b),(c,c)\}=I_A$,

进而有 $R^4=R^3\circ R=I_A\circ R=R$,$R^5=R^3\circ R^2=I_A\circ R^2=R^2$,继续该过程知,对于任意正整数 k 有 $R^{3k}=I_A$,$R^{3k+1}=R$,$R^{3k+2}=R^2$.

请注意,例 2-23 的结论不是偶然的,参见习题 2.2.

3. 函数 f 与函数 g 的复合 $f\circ g$

设 $f:A\to B$ 且 $g:B\to C$,函数 f 与函数 g 的复合记为 $f\circ g$. 由 2.1 节知 $f\subseteq A\times B$ 且 $g\subseteq B\times C$,关系 f 与关系 g 的复合也是记为 $f\circ g$. 它们是完全一致的.

2.2.4 关系的其他运算

在具体应用中,如在数据库理论中,还会涉及关系的其他运算[4,9],如关系的连接运算、关系的投影运算、关系的限制运算、关系的除运算等,由于篇幅限制和侧重点不同,在此不作讨论. 但为了后面讨论子格的方便,用较小的篇幅介绍关系限定运算中的一种特殊情况:关系在一个子集上的限定.

【定义 2-8】 设 R 是集合 A 上的关系,B 是 A 的子集,则 **R 在 B 上的限制**为

$$R|_B=\{(x,y)\mid x,y\in B\text{ 且 }(x,y)\in R\}$$

将 B 上的关系 $R|_B$ 仍记为 R.

【例 2-24】 设 $A=\{a,b,c,d,e,f,g\}$,A 上的关系 $R=I_A\cup\{(g,d),(g,b),(g,a),(d,b),(d,a),(g,e),(g,a),(e,a),(g,f),(g,c),(f,c),(f,a),(c,a)\}$,取 $B=\{a,b,c,d,g\}$,则 R 在 B 上的限制为

$$R|_B=I_B\cup\{(g,d),(g,b),(g,a),(d,b),(d,a),(g,a),(g,c),(c,a)\}$$

后面在讲了关系的性质后,还要学习关系的 3 种闭包运算,它们分别是自反闭包 $r(R)$、对称闭包 $s(R)$ 和传递闭包 $t(R)$.

在 C 语言中所出现的关系符号按数学方式写有小于“<”、小于等于“≤”、大于“>”、大于等于“≥”、等于“=”和不等于“≠”6 个符号. 所涉及的关系表达式[3]实际上是判断两个元

素是否有关系,因而有一个逻辑值.

思考 关系的计算机表示及关系运算如何实现?

习 题 2.2

1. 设 $A=\{0,1,2,3\}$,A 上的关系 R 和 S 分别为

$$R=\{(x,y)\mid x,y\in A,x+y=3\}$$
$$S=\{(x,y)\mid x,y\in A,y-x=1\}$$

试计算 $R\cup S,R\cap S,\bar{R},R-S,S-R,R\oplus S$.

2. 设 $R,S\subseteq A\times B$,则下列结论成立.

(1) $(R\cap S)^{-1}=R^{-1}\cap S^{-1}$.

(2) $(\bar{R})^{-1}=\overline{R^{-1}}$.

(3) $(R-S)^{-1}=R^{-1}-S^{-1}$.

(4) $(R\oplus S)^{-1}=R^{-1}\oplus S^{-1}$.

3. 设 $A=\{a,b,c,d\}$,A 上的关系 R 和 S 分别为

$$R=\{(b,b),(b,c),(c,a)\}$$
$$S=\{(b,a),(c,a),(c,d),(d,c)\}$$

试计算 $R^{-1},S^{-1},R\circ S,S\circ R,R^2,S^2,R\circ S\circ R,S\circ R^2$.

4. 设 R 是 A 上的关系,$\varnothing$是 A 上的空关系,证明 $R\circ\varnothing=\varnothing\circ R=\varnothing$.

5. 设 $R\subseteq A\times B,S,T\subseteq B\times C$,则 $R\circ(S\cup T)=(R\circ S)\cup(R\circ T)$,试证明之.

6. 设 $S,T\subseteq A\times B,R\subseteq B\times C$,则$(S\cap T)\circ R\subseteq(S\circ R)\cap(T\circ R)$,并举例说明不能将“$\subseteq$”改为“$=$”.

7. 设 $R\subseteq A\times B$,则

(1) $I_A\circ R=R$.

(2) $R\circ I_B=R$.

8. 设 R,S 和 T 为集合 A 上的关系,若 $S\subseteq T$,证明 $R\circ S\subseteq R\circ T$.

9. 设 $R\subseteq A\times A$,对于非负整数 m,有 $(R^m)^{-1}=(R^{-1})^m$.

10. 设$|A|=n$,R 是 A 上的关系,则存在自然数 i, j 使得 $R^i=R^j$,其中 $0\leqslant i<j\leqslant 2^{n^2}$.

11. 设 $A=\{a,b,c,d\}$,A 上的关系为 $R=\{(b,b),(b,c),(c,a)\}$,试计算 $\bigcup\limits_{n=1}^{\infty}R^n$.

12. 设 R 和 S 是集合 A 上的关系且 $R\circ S=I_A$.

(1) 若 A 是有限集合,则 R 和 S 都是 A 上的双射.

(2) 举例说明,若 A 是无限集合,则 R 和 S 不一定是 A 上的双射.

2.3 关系的性质

前面定义的关系是一般的关系,但在实际问题中,我们感兴趣的是具有某种或同时具有某几种特殊性质的关系.

对于集合 A 上的关系 $R\subseteq A\times A$,最常见的关系 R 的性质有 5 种,分别介绍如下.

2.3.1 自反性

【定义 2-9】 设 $R \subseteq A \times A$，若对于任意 $x \in A$，均有 $(x,x) \in R$，即 xRx，则称 R 为 A 上的**自反关系**，或称 R 在 A 上是自反的，或称 R 在集合 A 上具有自反性(reflexive property).

【例 2-25】 设 $A=\{a,b,c,d\}$，A 上的关系

$$R=\{(a,a),(a,b),(b,b),(c,c),(c,a),(d,d)\}$$

是自反的，因为对于任意 $x \in A$，均有 $(x,x) \in R$.

需要注意的是，R 是否为 A 上的自反关系，只需判断是否 A 中任意元素 x，x 与 x 都有关系 R. 于是，若 R 取为 $\{(a,a),(a,b),(b,b),(c,c),(c,a)\}$，则因为 $d \in A$，而 $(d,d) \notin R$，它不是自反的. 另外，若关系 R 取为 $R=\{(a,a),(b,b),(c,c),(c,a),(d,d)\}$，则它仍是自反的，它与 (a,b) 是否属于 R 无关.

整数集合 $\mathbf{Z}$ 上的整除关系"|"是自反的；集合 X 的幂集 $P(X)$ 上的包含关系"$\subseteq$"是自反的；实数集合 $\mathbf{R}$ 上的小于等于关系"$\leqslant$"是自反的；实数集合 $\mathbf{R}$ 上的小于关系"$<$"不是自反的.

下面的定理给出判断 R 自反的充要条件.

【定理 2-9】 设 $R \subseteq A \times A$，则 R 在 A 上自反的充要条件是 $I_A \subseteq R$，其中 I_A 是 A 上的恒等关系.

证 只需注意到 $I_A=\{(x,x) \mid x \in A\}$ 即可.

显然，空集 $\varnothing$ 上的关系只有空关系 $\varnothing$ 一个，该空关系 $\varnothing$ 是空集 $\varnothing$ 上的自反关系，因为 $A=\varnothing$，所以 $I_A=\varnothing$，而 $R=\varnothing$，这时有 $I_A \subseteq R$，故结论成立. 这是一种非常特殊的情况.

在关系图 G_R 中，若每一个点处都有一个环(自环)，则 R 是自反的，否则只要在某一个点处没有环，则 R 不是自反的. 例 2-25 所给 R 的关系如图 2-8 所示.

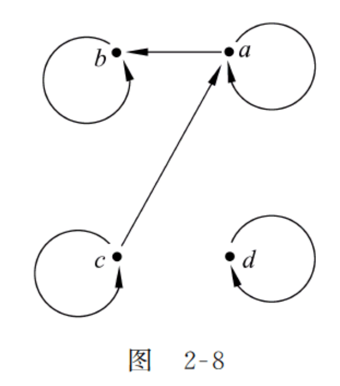


图 2-8

从 R 的关系矩阵 $\boldsymbol{M}_R$ 去判断，若 $\boldsymbol{M}_R$ 中主对角线元素全为 1，则 R 是自反的；若 $\boldsymbol{M}_R$ 中主对角线元素不全为 1(即至少有一个元素为 0)，则 R 不是自反的. 例 2-25 所给 R 的关系矩阵为

$$\boldsymbol{M}_R=\begin{bmatrix}1 & 1 & 0 & 0\\0 & 1 & 0 & 0\\1 & 0 & 1 & 0\\0 & 0 & 0 & 1\end{bmatrix}_{4\times 4}$$

对于初学者来说，关系性质的判定不是很容易的. 正确理解概念是至关重要的.

2.3.2 反自反性

【定义 2-10】 设 $R \subseteq A \times A$，若对于任意 $x \in A$，均有 $(x,x) \notin R$，则称 R 为 A 上的**反自反关系**，或称 R 在 A 上是反自反的，或称 R 在集合 A 上具有反自反性(irreflexive property).

【例 2-26】 设 $A=\{a,b,c,d\}$，A 上的关系

$$R=\{(b,a),(a,b),(b,c),(c,d),(c,a)\}$$

是反自反的，因为对于任意 $x \in A$，均有 $(x,x) \notin R$.

注意 R 是否为 A 上的反自反关系，只需判断是否 A 中任意元素 x，x 与 x 都没有关

系 R. 于是，在例 2-26 中，若 R 取为 $\{(a,a),(a,b),(b,c),(c,d),(c,a)\}$，则因为 $a\in A$，而 $(a,a)\in R$，它不是反自反的. 另外，若关系 R 取为 $\{(b,a),(b,c),(c,d),(c,a)\}$，则它仍是反自反的，它与 (a,b) 是否属于 R 无关.

整数集合 $\mathbf{Z}$ 上的整除关系"|"不是反自反的；集合 X 的幂集 $P(X)$ 上的包含关系"$\subseteq$"不是反自反的；实数集合 $\mathbf{R}$ 上的小于等于关系"$\leqslant$"不是反自反的；实数集合 $\mathbf{R}$ 上的小于关系"$<$"是反自反的.

下面的定理给出判断 R 反自反的充要条件.

【定理 2-10】 设 $R\subseteq A\times A$，则 R 在 A 上反自反的充要条件是 $I_A\cap R=\varnothing$，其中 I_A 是 A 上的恒等关系.

证 （留作练习）.

显然，空集 $\varnothing$ 上的空关系 $\varnothing$ 也是其上的反自反关系，因为 $A=\varnothing$，所以 $I_A=\varnothing$，而 $R=\varnothing$，这时有 $I_A\cap R=\varnothing$，故结论成立. 于是，空集 $\varnothing$ 上的空关系 $\varnothing$ 既是自反的，也是反自反的. 下面所举的关系既不是自反的，也不是反自反的.

【例 2-27】 设 $A=\{a,b,c,d\}$，A 上的关系

$$R=\{(a,a),(a,b),(b,b),(c,d),(c,a)\}$$

因为对于 $c\in A$，有 $(c,c)\notin R$，所以 R 不是自反的；因为 $a\in A$，有 $(a,a)\in R$，所以 R 不是反自反的.

例 2-25 给出的是自反但不是反自反的关系例子，例 2-26 给出的是反自反但不是自反的关系例子.

在关系图 G_R 中，若每一个点处都没有环，则 R 是反自反的，否则只要在某一个点处有环，则 R 不是反自反的. 例 2-26 所给 R 的关系图，如图 2-9 所示.

图 2-9

从 R 的关系矩阵 $\boldsymbol{M}_R$ 去判断，若 $\boldsymbol{M}_R$ 中主对角线元素全为 0，则 R 是反自反的；若 $\boldsymbol{M}_R$ 中主对角线元素不全为 0(即至少有一个元素为 1)，则 R 不是反自反的. 例 2-26 所给 R 的关系矩阵为

$$\boldsymbol{M}_R=\begin{bmatrix}0&1&0&0\\1&0&1&0\\1&0&0&1\\0&0&0&0\end{bmatrix}_{4\times 4}$$

2.3.3 对称性

【定义 2-11】 设 $R\subseteq A\times A$，对于任意 $x,y\in A$，如果 $(x,y)\in R$，那么有 $(y,x)\in R$，则称 R 为 A 上的**对称关系**，或称 R 在 A 上是对称的，或称 R 在集合 A 上具有对称性(symmetric property).

【例 2-28】 设 $A=\{a,b,c,d\}$，A 上的关系

$$R=\{(b,a),(a,b),(b,b),(d,c),(c,d)\}$$

是对称的.

关系 R 为 A 上的对称关系，必须满足：只要 $(x,y)\in R$，就一定有 $(y,x)\in R$. 于是，I_A 中的元素不影响关系 R 的对称性. 在例 2-28 中，若 R 取为 $\{(b,a),(a,b),(b,b),(d,c)\}$，则因为 $(d,c)\in R$，而 $(c,d)\notin R$，它不是对称的.

整数集合 **Z** 上的整除关系"|"不是对称的；集合 $X(|X|\geqslant 1)$ 的幂集 $P(X)$ 上的包含关系"$\subseteq$"不是对称的；实数集合 **R** 上的小于等于关系"$\leqslant$"不是对称的；实数集合 **R** 上的小于关系"$<$"不是对称的；三角形之间的全等关系"$\cong$"是对称关系；整数集 **Z** 上的模 k 同余关系"$\equiv_k$"具有对称性.

下面的定理给出判断 R 是对称的充要条件.

【定理 2-11】 设 $R\subseteq A\times A$，则 R 在 A 上对称的充要条件是 $R=R^{-1}$.

证 （留作练习）.

在关系图中 G_R 中，若每一对不同点之间有边，即有向曲线，一定是成对出现的，则 R 是对称的，否则只要在某一对点处没有成对出现，则 R 不是对称的. 例 2-28 所给 R 的关系图如图 2-10 所示.

显然，R 对称充要条件是 $\boldsymbol{M}_R$ 中元素关于主对角线对称，即 $\boldsymbol{M}_R$ 对称. 例 2-28 所给 R 的关系矩阵为

$$\boldsymbol{M}_R=\begin{bmatrix}0&1&0&0\\1&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}_{4\times 4}$$

图 2-10

2.3.4 反对称性

【定义 2-12】 设 $R\subseteq A\times A$，对于任意 $x,y\in A$，如果 $(x,y)\in R$ 且 $(y,x)\in R$，那么一定有 $x=y$，则称 R 为 A 上的**反对称关系**，或称 R 在 A 上是反对称的，或称 R 在集合 A 上具有反对称性(antisymmetric property).

关系 R 反对称的等价定义为：R 为 A 上的反对称关系是指对于任意 $x,y\in A$，若 $x\neq y$，则 $(x,y)\in R$ 与 $(y,x)\in R$ 不能同时成立.

【例 2-29】 设 $A=\{a,b,c,d\}$，A 上的关系

$$R=\{(a,a),(a,b),(b,b),(b,c),(d,c)\}$$

是反对称的.

根据反对称关系的定义知，I_A 中的元素不影响其反对称性，像例 2-29 中的 (a,a)，(b,b). 关系 R 反对称，则 A 中任意两个不同元素 x，y，$(x,y)\in R$ 与 $(y,x)\in R$ 不能同时成立，当然可以都不成立：$(x,y)\notin R$ 且 $(y,x)\notin R$. 若 R 取为 $\{(a,a),(a,b),(b,b),(b,c),(c,b)\}$，则因为 $b,c\in A$，$b\neq c$，而 $(b,c)\in R$ 且 $(c,b)\in R$，因此，R 不是反对称的；同时，这样取的关系 R 也不是对称的，因为 $(a,b)\in R$，但 $(b,a)\notin R$. 例 2-28 给出的是对称但不是反对称的关系例子，例 2-29 给出的是反对称但不是对称的关系例子. 再看一个例子.

【例 2-30】 设 $A=\{a,b,c,d\}$，A 上的关系

$$R=\{(a,a),(c,c)\}$$

既是对称的，也是反对称的.

整数集合 **Z** 上的整除关系"|"不是反对称的，因为 $2|-2$ 且 $-2|2$；X 的幂集 $P(X)$ 上的包含关系"$\subseteq$"是反对称的，因为对于任意 $A,B\in P(X)$，若 $A\subseteq B$ 且 $B\subseteq A$，一定有 $A=B$；实数集合 **R** 上的小于等于关系"$\leqslant$"是反对称的；实数集合 **R** 上的小于关系"$<$"是反对称的，因为对于任意 $x,y\in\mathbf{R}$，若 $x\neq y$，则 $x<y$ 和 $y<x$ 不会同时成立.

下面的定理给出判断 R 反对称的充要条件.

【定理 2-12】 设 $R\subseteq A\times A$,则 R 在 A 上反对称的充要条件是 $R\cap R^{-1}\subseteq I_A$,其中 I_A 是 A 上的恒等关系.

证 (1) 假定 R 反对称. 若 $(x,y)\in R\cap R^{-1}$,则 $(x,y)\in R$ 且 $(x,y)\in R^{-1}$. 由 $(x,y)\in R^{-1}$ 可得出 $(y,x)\in R$. 由 R 反对称知,$x=y$,这时有 $(x,y)\in I_A$,于是 $R\cap R^{-1}\subseteq I_A$.

(2) 假定 $R\cap R^{-1}\subseteq I_A$. 对任意 $x,y\in A$,若 $(x,y)\in R$ 且 $(y,x)\in R$,由 $(y,x)\in R$ 可推出 $(x,y)\in R^{-1}$,所以 $(x,y)\in R\cap R^{-1}$. 而 $R\cap R^{-1}\subseteq I_A$,于是 $(x,y)\in I_A$,进而 $x=y$. 根据反对称的定义知, R 反对称.

在关系图 G_R 中,若每一对不同点处的边都没有成对出现,则 R 是反对称的,否则只要在某一对点处的边成对出现,则 R 不是反对称的. 例 2-29 所给 R 的关系图如图 2-11 所示.

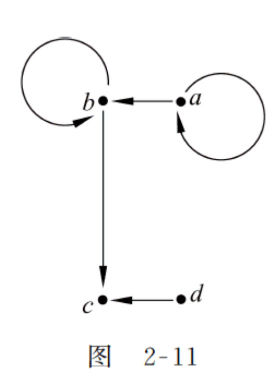


图 2-11

关系 R 反对称的充要条件是关系矩阵 $\boldsymbol{M}_R$ 中关于主对角线对称的元素不能同时为 1. 例 2-29 所给 R 的关系矩阵为

$$\boldsymbol{M}_R=\begin{bmatrix}1&1&0&0\\0&1&1&0\\0&0&0&0\\0&0&1&0\end{bmatrix}_{4\times4}$$

2.3.5 传递性

【定义 2-13】 设 $R\subseteq A\times A$,对于任意 $x,y,z\in A$,如果 $(x,y)\in R$ 且 $(y,z)\in R$,那么 $(x,z)\in R$,则称 R 为 A 上的**传递关系**,或称 R 在 A 上是传递的,或称 R 在集合 A 上具有传递性(transitive property).

【例 2-31】 设 $A=\{a,b,c,d\}$,A 上的关系

$$R=\{(a,a),(a,b),(b,b),(b,c),(a,c),(c,a)\}$$

是不传递的, 因为 $(c,a)\in R$ 且 $(a,c)\in R$,但 $(c,c)\notin R$.

【例 2-32】 设 $A=\{a,b,c,d\}$,A 上的关系

$$R=\{(a,a),(a,b),(b,b),(b,c),(c,b),(a,c),(c,a),(c,c),(b,a)\}$$

是传递的.

根据传递关系的定义,只要 $(x,y)\in R$ 且 $(y,z)\in R$,就一定有 $(x,z)\in R$,则 R 是传递的. 在例 2-31 中,虽然 $(a,b)\in R$ 且 $(b,c)\in R$,有 $(a,c)\in R$;甚至 $(a,c)\in R$ 且 $(c,a)\in R$,有 $(a,a)\in R$,但因为 $(c,a)\in R$ 且 $(a,c)\in R$,但 $(c,c)\notin R$,所以 R 不传递.

整数集合 $\mathbf{Z}$ 上的整除关系"|"是传递的;集合 X 的幂集 $P(X)$ 上的包含关系"$\subseteq$"是传递关系;实数集合 $\mathbf{R}$ 上的小于等于关系"$\leqslant$"是传递的;实数集合 $\mathbf{R}$ 上的小于关系"$<$"是传递的.

下面的定理给出判断 R 传递的充要条件.

【定理 2-13】 设 $R\subseteq A\times A$,则 R 在 A 上传递的充要条件是 $R\circ R\subseteq R$.

证 ($\Rightarrow$)对于任意 $(x,z)\in R\circ R$,由关系复合运算的定义知,存在 $y\in A$ 使得 $(x,y)\in R$ 且 $(y,z)\in R$. 因为 R 传递,所以 $(x,z)\in R$, 于是 $R\circ R\subseteq R$.

($\Leftarrow$)对于任意 $x,y,z\in A$,设 $(x,y)\in R$ 且 $(y,z)\in R$,由关系复合运算的定义知

$(x,z)\in R\circ R$. 因为 $R\circ R\subseteq R$,所以$(x,z)\in R$,故 R 传递.

【例 2-33】 设 $A=\{a,b,c,d\}$,A 上的关系

$$R=\{(a,b),(a,c)\}$$

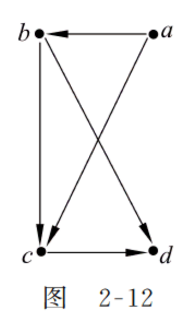


图 2-12

是传递的,因为经计算知 $R\circ R=\varnothing$,显然有 $R\circ R\subseteq R$. 值得特别注意的是,不能因为$(a,b)\in R$,而没有$(b,c)\in R$ 之类,就认为 R 不传递. 若取

$$R=\{(a,b)\}$$

则 R 也是传递的.

在关系图 G_R 中,对任意的 $x,y,z\in A$,只要 x 到 y 有边且 y 到 z 有边,就一定有 x 到 z 有边,则 R 是传递的. 假设关系 R 的关系如图 2-12 所示,则关系 R 不传递,因为 a 到 c 有边且 c 到 d 有边,但 a 到 d 没有边.

根据定理 2-13,考虑 $R\circ R$ 的关系矩阵与 R 的关系矩阵的关系可得出从 R 的关系矩阵 $\boldsymbol{M}_R$ 去判断 R 的传递性的方法.

上面介绍的是常见的 5 种关系的性质,在实际问题中可能会遇到其他性质的关系(如连续性、Euclid 性、连通性、反传递性、循环性等,部分性质参见习题 2.3). 下面的例子是根据所给定的关系,判断 R 具有何性质. 当然,可以考虑让计算机判断关系具有哪些性质.

【例 2-34】 设 $A=\{0,1,2,3,4,5\}$,A 上的关系

$$R=\{(x,y)\mid x,y\in A,x+y=5\}$$

试判断 R 具有的性质(自反、反自反、对称、反对称和传递),说明理由.

解 (1) R 不具有自反性:$(0,0)\notin R$.

(2) R 具有反自反性:任意 $x\in A$,显然有$(x,x)\notin R$.

(3) R 具有对称性:任意 $x,y\in A$,若$(x,y)\in R$,则 $x+y=5$,显然 $y+x=5$,即$(y,x)\in R$.

(4) R 不具有反对称性:$(2,3)\in R$,$(3,2)\in R$.

(5) R 不具有传递性:因为$(2,3)\in R$,$(3,2)\in R$,但$(2,2)\notin R$.

综上所述,R 具有反自反性和对称性(事实上,可以先求出 R,再讨论其性质).

【例 2-35】 设 R 是集合 A 上的对称且传递的关系,可得出 R 是集合 A 上的自反关系吗?

有人做如下推导:对于任意 $x\in A$,由于 R 是对称的,则由$(x,y)\in R$ 可得出$(y,x)\in R$,又因为 R 是传递的,由$(x,y)\in R$ 及$(y,x)\in R$ 可得出$(x,x)\in R$,所以 R 是自反的. 请举例指出上述推理的错误之处.

解 取 $A=\{a,b,c\}$,令 $R=\{(a,a),(a,b),(b,a),(b,b)\}$,容易知道 R 是集合 A 上的对称的、传递的关系. 由于 $c\in A$,而$(c,c)\notin R$,因此 R 不是 A 上的自反关系.

上述推理错在对 R 是 A 上的对称关系的理解上. R 是 A 上的对称关系是指,对于任意 $x,y\in A$,如果$(x,y)\in R$,那么可得出$(y,x)\in R$. 若“$(x,y)\in R$”不成立,则上述推理失效.

最后考察关系的性质与关系运算之间的关系.

【例 2-36】 设 R,S 是集合 A 上的传递关系,试判断$R\circ S$是否一定传递,说明理由. $R\circ R$ 是否一定传递?

解 $R\circ S$ 不一定传递. 例如,取 $A=\{a,b,c,d\}$,令

$$R=\{(a,b),(b,c),(a,c)\},\quad S=\{(b,c),(c,a),(b,a)\}$$

很容易验证，R,S 是集合 A 上的传递关系. 而

$$R\circ S=\{(a,c),(a,a),(b,a)\}$$

因为

$$(b,a)\in R\circ S,(a,c)\in R\circ S$$

但 $(b,c)\notin R\circ S$，因此 $R\circ S$ 不传递.

由于 R 是传递的，于是 $R\circ R\subseteq R$，因此 $(R\circ R)\circ(R\circ R)\subseteq R\circ R$，所以 $R\circ R$ 是传递的.

表 2-2 列举出关系的性质与关系运算之间的关系，表中"√"表示正确(True)，"×"表示错误(False).

表 2-2

运算 \ 性质	自反性	反自反性	对称性	反对称性	传递性
$R\cap S$	√	√	√	√	√
$R\cup S$	√	√	√	×	×
$R-S$	×	√	√	√	×
R^{-1}	√	√	√	√	√
$R\circ S$	√	×	×	×	×

【例 2-37】 设 R,S 是集合 A 上的对称关系.

(1) 举例说明 $R\circ S$ 不一定对称.

(2) 证明：$R\circ S$ 对称的充要条件是 $R\circ S=S\circ R$.

解 (1) 例如，取 $A=\{a,b,c\}$，令

$$R=\{(a,b),(b,a)\},\quad S=\{(b,c),(c,b)\}$$

显然，R,S 是集合 A 上的对称关系. 而 $R\circ S=\{(a,c)\}$，因为 $(a,c)\in R\circ S$，但 $(c,a)\notin R\circ S$，因此 $R\circ S$ 不对称.

(2) 由于 R,S 对称，所以 $R^{-1}=R$，且 $S^{-1}=S$.

($\Rightarrow$)若 $R\circ S$ 对称，则 $(R\circ S)^{-1}=R\circ S$，而 $(R\circ S)^{-1}=S^{-1}\circ R^{-1}=S\circ R$，因此 $R\circ S=S\circ R$.

($\Leftarrow$)若 $R\circ S=S\circ R$，因为 $(R\circ S)^{-1}=S^{-1}\circ R^{-1}=S\circ R$，进而 $(R\circ S)^{-1}=R\circ S$，于是 $R\circ S$ 对称.

习　题　2.3

1. 设 $R\subseteq A\times A$，证明 R 在 A 上是反自反的充要条件是 $I_A\cap R=\varnothing$，其中 I_A 是 A 上的恒等关系.

2. 设 $R\subseteq A\times A$，证明 R 在 A 上对称的充要条件是 $R=R^{-1}$.

3. 设 $A=\{a,b,c\}$，A 上的关系 $R=\{(a,b),(b,c)\}$，试求出 3 个包含关系 R 的传递关系.

4. 设 $R\subseteq A\times A$,对于任意 $x,y,z\in A$,如果$(x,y)\in R$ 且$(y,z)\in R$,那么$(x,z)\notin R$,则称 R 为 A 上的**反传递关系**.

(1) 试举出一个反传递关系的例子.

(2) 证明:R 反传递的充要条件是$(R\circ R)\cap R=\varnothing$.

5. 设 $R\subseteq A\times A$,对于任意 $x,y,z\in A$,如果$(x,y)\in R$ 且$(y,z)\in R$,那么$(z,x)\in R$,则称 R 为 A 上的**循环关系**.

(1) 试举出一个循环关系的例子.

(2) 证明:若 R 是自反的和循环的,则 R 具有对称性和传递性.

6. 若$|A|=n$,R 为 A 上的反对称关系,求出 $R\cap R^{-1}$ 的关系矩阵中至少多少个元素是 0.

7. 设 $R\subseteq A\times A$,若 R 具有自反性及传递性,则 $R\circ R=R$. 其逆命题为真吗?

8. 设 R 是复数集合 $\mathbf{C}$ 上的关系,定义如下:

$$R=\{(x,y)\mid x,y\in\mathbf{C}\text{ 且 }x-y=a+b\mathrm{i},\text{其中 }a,b\text{ 为非负整数}\}$$

试确定 R 的性质(自反、反自反、对称、反对称和传递),说明理由.

9. 确定三角形之间的相似关系"∽"具有哪些性质(自反、反自反、对称、反对称和传递),说明理由.

10. 设 $X\neq\varnothing$,R 是 $P(X)$上的关系,定义如下:

$$R=\{(A,B)\mid A,B\in P(X)\text{ 且 }A\cap B\neq\varnothing\}$$

试确定 R 的性质(自反性、反自反性、对称性、反对称性和传递性),说明理由.

11. 设 $A=\{a,b,c,d\}$,试举出一个 A 上的关系的例子,使其同时不具有自反性、反自反性、对称性、反对称性和传递性.

12. 设 R,S 是集合 A 上的关系,试判断下列命题的真假,说明理由.

(1) R 和 S 是自反的,则 $R\cup S$ 自反.

(2) R 和 S 是反自反的,则 $R\cup S$ 反自反.

(3) R 和 S 是对称的,则 $R\cup S$ 对称.

(4) R 和 S 是反对称的,则 $R\cup S$ 反对称.

(5) R 和 S 是传递的,则 $R\cup S$ 传递.

2.4 关系的闭包

通过关系的一些运算可以得到新的关系. 对于 A 上的关系 R,希望 R 具有某些有用的性质,如自反性. 若 R 不具有自反性,通过在 R 中添加一些有序对使其变成自反关系,这样也可以得到一些新的 A 上的关系.

2.4.1 自反闭包 $r(R)$

先看下面的例子.

【例 2-38】 设 $A=\{a,b,c\}$,A 上的关系 $R=\{(a,a),(b,a),(b,c),(c,a),(a,c)\}$,试求出所有的包含 R 的自反关系.

解 下面的 4 个关系都是包含 R 的自反关系:

$$R_1 = R \cup \{(b,b),(c,c)\} = \{(a,a),(b,a),(b,c),(c,a),(a,c),(b,b),(c,c)\}$$

$$R_2 = R \cup \{(b,b),(c,c),(a,b)\}$$
$$= \{(a,a),(b,a),(b,c),(c,a),(a,c),(b,b),(c,c),(a,b)\}$$

$$R_3 = R \cup \{(b,b),(c,c),(c,b)\}$$
$$= \{(a,a),(b,a),(b,c),(c,a),(a,c),(b,b),(c,c),(c,b)\}$$

$$R_4 = R \cup \{(b,b),(c,c),(a,b),(c,b)\}$$
$$= \{(a,a),(b,a),(b,c),(c,a),(a,c),(b,b),(c,c),(a,b),(c,b)\}$$

从 R_1,R_2,R_3 和 R_4 可以看出,对于包含关系"$\subseteq$"来说,R_1 是 4 个包含 R 的自反关系中最小的,即有 $R_1 \subseteq R_i(i=1,2,3,4)$.就把 R_1 称为 R 的自反闭包.

【定义 2-14】 设 $R \subseteq A \times A$,最小的包含 R 的自反关系称为 R 的**自反闭包**(reflexive closure),记为 $r(R)$.

从定义 2-14 可知,R 的自反闭包 $r(R)$是 A 上的关系,且必须满足以下 3 个条件:

(1) 包含 R;

(2) 自反性;

(3) 最小性.

在计算 R 的自反闭包 $r(R)$时,为了保证最小性,在关系 R 的基础上尽可能少地添加元素,但要求自反.实际上,只要把 A 上的恒等关系 I_A 中的全部元素加进去就可以了,可以证明:

【定理 2-14】 设 $R \subseteq A \times A$,则 $r(R) = R \cup I_A$.

证 (1) 显然 $R \cup I_A$ 包含 R.

(2) 因为 $I_A \subseteq R \cup I_A$,所以 $R \cup I_A$ 自反.

(3) 对于任意的包含 R 的自反关系 R',有 $R \subseteq R'$ 且 $I_A \subseteq R'$,进而有 $R \cup I_A \subseteq R'$.

故,$R \cup I_A$ 是最小的包含 R 的自反关系,即自反闭包.

很容易从关系 R 的关系图,得出其自反闭包 $r(R)$的关系图.

【例 2-39】 设 $A=\{a,b,c,d\}$,A 上的关系 R 的关系图 G_R 如图 2-13 所示,试画出 R 的自反闭包 $r(R)$的关系图 $G_{r(R)}$.

解 要画出 R 的自反闭包 $r(R)$的关系图 $G_{r(R)}$,在 R 的关系图 G_R 的基础上,只需在每一个点处都画上一个环即可,如图 2-14 所示.

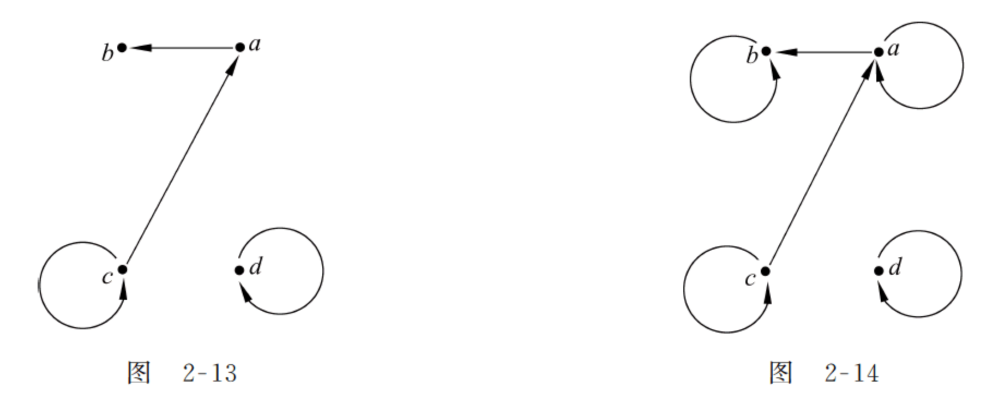


图 2-13　　　　图 2-14

除关系 R 的自反闭包外,还经常考虑 R 的对称闭包和传递闭包.

2.4.2　对称闭包 $s(R)$

【定义 2-15】　设 $R\subseteq A\times A$,最小的包含 R 的对称关系称为 R 的**对称闭包**(symmetric closure),记为 $s(R)$.

计算 R 的对称闭包 $s(R)$ 时,在关系 R 的基础上尽可能少地添加元素,只要对称就可以了.实际上,把 R 的逆关系 R^{-1} 中的全部元素加进去就可以了,可以证明:

【定理 2-15】　设 $R\subseteq A\times A$,则 $s(R)=R\cup R^{-1}$.

证　(留作练习).

【例 2-40】　设 $A=\{a,b,c\}$,A 上的关系 $R=\{(a,a),(b,a),(b,c),(c,a),(a,c)\}$,试求出 R 的对称闭包 $s(R)$.

解　$s(R)=R\cup R^{-1}=\{(a,a),(b,a),(b,c),(c,a),(a,c)\}$

$\cup\{(a,a),(a,b),(c,b),(a,c),(c,a)\}$

$=\{(a,a),(b,a),(b,c),(c,a),(a,c),(a,b),(c,b)\}$

要画出 R 的对称闭包 $s(R)$ 的关系图 $G_{s(R)}$,在 R 的关系图 G_R 的基础上,若一对不同点之间有边,则必须成对出现.

【例 2-41】　设 $A=\{a,b,c,d\}$,A 上的关系 R 的关系图 G_R 如图 2-13 所示,试画出 R 的对称闭包 $s(R)$ 的关系图 $G_{s(R)}$.

解　R 的对称闭包 $s(R)$ 的关系图 $G_{s(R)}$ 如图 2-15 所示.

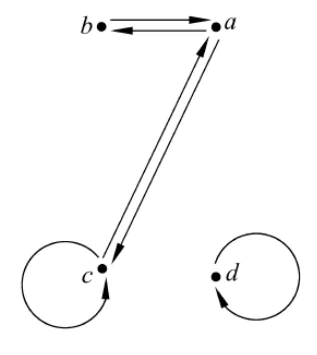


图　2-15

2.4.3　传递闭包 $t(R)$

【定义 2-16】　设 $R\subseteq A\times A$,最小的包含 R 的传递关系称为 R 的**传递闭包**(transitive closure),记为 $t(R)$.

【例 2-42】　设 $A=\{a,b,c\}$,A 上的关系 $R=\{(a,b),(b,c),(b,a)\}$,试求出 R 的传递闭包 $t(R)$.

解　$t(R)=\{(a,b),(b,c),(b,a),(a,c),(a,a),(b,b)\}$.

注意　在根据定义计算传递闭包 $t(R)$ 时,同样是尽可能少地添加元素,但要保证添加后得到的关系是传递的.在例 2-42 中,不能仅因为 $(a,b),(b,c)\in R$,添加元素 (a,c) 就可以了,因为这样的话,所得到的关系 $\{(a,b),(b,c),(b,a),(a,c)\}$ 是不传递的,还要添加 $(a,a),(b,b)$,这是初学者容易出错的地方.建议在做完后要检查是否传递.

【例 2-43】　设 $A=\{a,b,c,d\}$,A 上的关系 R 的关系图 G_R 如图 2-13 所示,试画出 R 的传递闭包 $t(R)$ 的关系图 $G_{t(R)}$.

解　R 的传递闭包 $t(R)$ 的关系图 $G_{t(R)}$ 如图 2-16 所示.

计算传递闭包的一般公式是比较复杂的.

【定理 2-16】　设 $R\subseteq A\times A$,则 $t(R)=\bigcup\limits_{i=1}^{\infty}R^i=R\cup R^2\cup R^3\cup\cdots$.

证　为讨论方便起见,令 $R^+=\bigcup\limits_{i=1}^{\infty}R^i=R\cup R^2\cup R^3\cup\cdots$下面证明 $t(R)=R^+$.

(1) R^+ 是传递的.对于任意 $x,y,z\in A$,假设 $(x,y)\in R^+$ 且 $(y,z)\in R^+$,根据并运算的定义知,存在正整数 r,s,使得 $(x,y)\in R^r$,$(y,z)\in R^s$,于是有 $(x,z)\in R^r\circ R^s=R^{r+s}\subseteq R^+$,所以

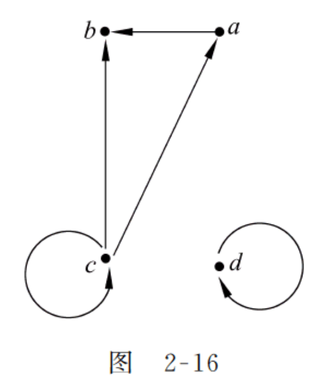


图 2-16

R^+ 是传递的. 显然 $R\subseteq R^+$，由传递闭包的定义知，$t(R)\subseteq R^+$.

(2) 因为 $R\subseteq t(R)$，使用数学归纳法可以证明：

$$R^i \subseteq t(R),\quad i=1,2,3,\cdots$$

假定 $R^i\subseteq t(R)$，任取 $(x,y)\in R^{i+1}=R^i\circ R$，存在元素 $a\in A$ 使得 $(x,a)\in R^i$ 且 $(a,y)\in R$；由归纳假定有 $R^i\subseteq t(R)$，而 $R\subseteq t(R)$，所以 $(x,a)\in t(R)$，$(a,y)\in t(R)$；根据 $t(R)$ 传递知，$(x,y)\in t(R)$，于是 $R^{i+1}\subseteq t(R)$. 因为 $R^i\subseteq t(R)$，$i=1,2,3,\cdots$ 所以 $R\cup R^2\cup R^3\cup\cdots=R^+\subseteq t(R)$.

由(1)和(2)，有 $t(R)=R^+$. 证毕.

定理 2-16 不适合于计算传递闭包，因为要计算 R^i，$i=1,2,3,\cdots$，是不现实的. 但在集合 A 中元素有限时，下面的定理是有用的.

先介绍鸽笼原理，又称为抽屉原理，其结论是显然的，它主要用于得出具有某种性质的元素是存在的.

鸽笼原理(pigeonhole principle) $n+1$ 或更多只鸽子飞进 n 个笼子时，一定有一个笼子里面至少两只鸽子.

抽屉原理 $n+1$ 或更多个苹果放进 n 个抽屉时，一定有一个抽屉里面至少两只苹果.

推广的鸽笼原理(extended pigeonhole principle) n 只鸽子飞进 m 个笼子时，一定有一个笼子里面至少 $\left\lceil \frac{n}{m} \right\rceil$ 只鸽子.

【定理 2-17】 设 $|A|=n$，$R\subseteq A\times A$，则 $t(R)=\bigcup_{i=1}^{n} R^i = R\cup R^2\cup\cdots\cup R^n$.

证 设 $(x,y)\in t(R)$，由定理 2-16 知，存在正整数 p 使得 $(x,y)\in R^p$，不妨设 p 是满足该条件最小的. 根据 R^p 的定义，存在集合 A 中的元素 $x,e_1,e_2,\cdots,e_{p-1},e_p=y$，满足

$$(x,e_1)\in R,(e_1,e_2)\in R,\cdots,(e_{p-1},e_p)\in R$$

假定 $p>n$，因为 $|A|=n$，由于 $\left\lceil \frac{p}{n} \right\rceil>1$，根据推广的鸽笼原理，$e_1,e_2,\cdots,e_{p-1},e_p$ 中必存在相同元素 $e_r=e_s$，$1\leqslant r<s\leqslant p$. 因此，有

$$(x,e_1)\in R,\cdots,(e_{r-1},e_r)\in R,\cdots,(e_r,e_{s+1})\in R,\cdots,(e_{p-1},y)\in R$$

再根据复合运算的定义知，$(x,y)\in R^{r+(p-s)}=R^{p-(s-r)}$. 因为 $p-(s-r)<p$，与 p 的最小性矛盾，故 $p>n$ 不成立. 证毕.

当 $A=\varnothing$ 时，有 $R=\varnothing$，于是显然有 $t(R)=\varnothing$.

【例 2-44】 利用定理 2-17 重新计算例 2-42 中 R 的传递闭包 $t(R)$.

解 因为 $R=\{(a,b),(b,c),(b,a)\}$，所以有

$$R^2=\{(a,c),(a,a),(b,b)\}$$

$$R^3=R\circ R^2=\{(a,b),(b,c),(b,a)\}$$

因此，$t(R)=R\cup R^2\cup R^3=\{(a,b),(b,c),(b,a),(a,c),(a,a),(b,b)\}$.

根据定理 2-17，可以得出由关系矩阵 $\boldsymbol{M}_R$ 求传递闭包的关系矩阵 $\boldsymbol{M}_{t(R)}$ 的方法. 但当集合 A 中元素较多时很繁琐，为此 Warshall 在 1962 年提出了一个求传递闭包的有效算法[8, 9, 11].

最后考虑闭包运算与其他内容的联系.

1. 关系的闭包运算与其他运算之间的联系

下述定理给出了关系的闭包运算与关系的并运算之间的一些结论.

【定理 2-18】 设 $R_1 \subseteq A \times A, R_2 \subseteq A \times A$,则

(1) $r(R_1 \cup R_2) = r(R_1) \cup r(R_2)$;

(2) $s(R_1 \cup R_2) = s(R_1) \cup s(R_2)$;

(3) $t(R_1 \cup R_2) \supseteq t(R_1) \cup t(R_2)$.

证 只证明(2)和(3),(1)留作练习.

(2) $s(R_1 \cup R_2) = (R_1 \cup R_2) \cup (R_1 \cup R_2)^{-1} = (R_1 \cup R_2) \cup (R_1^{-1} \cup R_2^{-1})$

$= (R_1 \cup R_1^{-1}) \cup (R_2 \cup R_2^{-1}) = s(R_1) \cup s(R_2)$.

(3) 由定理 2-16 知, $t(R_1) = \bigcup_{i=1}^{\infty} R_1^i = R_1 \cup R_1^2 \cup R_1^3 \cup \cdots$

$$t(R_2) = \bigcup_{i=1}^{\infty} R_2^i = R_2 \cup R_2^2 \cup R_2^3 \cup \cdots$$

$$t(R_1 \cup R_2) = \bigcup_{i=1}^{\infty} (R_1 \cup R_2)^i = (R_1 \cup R_2) \cup (R_1 \cup R_2)^2 \cup (R_1 \cup R_2)^3 \cup \cdots$$

显然,由关系运算的性质有$(R_1 \cup R_2)^i \supseteq R_1^i \cup R_2^i$,于是 $t(R_1 \cup R_2) \supseteq t(R_1) \cup t(R_2)$.

下面的例 2-45 说明,在定理 2-18(3)中,不能把“$\supseteq$”改为“$=$”.

【例 2-45】 试举例说明 $t(R_1 \cup R_2) \neq t(R_1) \cup t(R_2)$.

解 设 $A = \{a, b, c\}$, 令 $R_1 = \{(a,b),(b,c)\}, R_2 = \{(b,a)\}$,这时 $t(R_1) = \{(a,b),(b,c),(a,c)\}, t(R_2) = \{(b,a)\}$,所以

$$t(R_1) \cup t(R_2) = \{(a,b),(b,c),(a,c),(b,a)\}$$

而由前面例子的结果知,$t(R_1 \cup R_2) = \{(a,b),(b,c),(a,c),(b,a),(a,a),(b,b)\}$, 因此,有 $t(R_1 \cup R_2) \neq t(R_1) \cup t(R_2)$.

2. 闭包运算与关系的性质的联系

【定理 2-19】 设 $R \subseteq A \times A$,

(1) 若 R 自反,则 $s(R)$及 $t(R)$也自反;

(2) 若 R 对称,则 $r(R)$及 $t(R)$也对称;

(3) 若 R 传递,则 $r(R)$也传递,而 $s(R)$不一定传递.

证 只证明(2)和(3),(1)留作练习.

(2) 由已知 R 对称,有 $R = R^{-1}$. 由于 $r(R) = R \cup I_A$,而$(r(R))^{-1} = (R \cup I_A)^{-1} = R^{-1} \cup I_A^{-1} = R \cup I_A = r(R)$,所以 $r(R)$对称.

因为 R 对称,所以$(R^i)^{-1} = (R^{-1})^i = R^i$. 由于 $t(R) = \bigcup_{i=1}^{\infty} R^i = R \cup R^2 \cup R^3 \cup \cdots$于是

$$(t(R))^{-1} = (R \cup R^2 \cup R^3 \cup \cdots)^{-1} = R^{-1} \cup (R^2)^{-1} \cup (R^3)^{-1} \cup \cdots$$
$$= R \cup R^2 \cup R^3 \cup \cdots = t(R)$$

故 $t(R)$也对称.

(3) 因为 R 传递,所以 $R \circ R \subseteq R$. 而 $r(R) = R \cup I_A$,这时

$$r(R) \circ r(R) = (R \cup I_A) \circ (R \cup I_A) = R \circ (R \cup I_A) \cup I_A \circ (R \cup I_A)$$

$$=R \circ R \cup R \circ I_A \cup I_A \circ (R \cup I_A)$$
$$=R \circ R \cup R \cup (R \cup I_A) \subseteq R \cup R \cup (R \cup I_A)$$
$$=R \cup I_A = r(R)$$

因此，有 $r(R)$ 传递.

例如，$A=\{a,b,c\}$，$R=\{(a,b)\}$，显然 R 传递. 而 $s(R)=\{(a,b),(b,a)\}$不传递.

列举关系的性质与闭包运算的联系如表 2-3 所示.

表　2-3

性质 / 运算	自反性	反自反性	对称性	反对称性	传递性
$r(R)$	√	×	√	√	√
$s(R)$	√	√	√	×	×
$t(R)$	√	×	√	×	√

3. 多重闭包运算

由于关系的闭包运算在计算机其他专业课中很有用，下面再对多重闭包问题进行简单讨论.

对于多重闭包运算，规定从右至左依次进行运算，如

$$tsr(R) = t(s(r(R)))$$

很容易知道，$rt(R)=r(R\cup R^2\cup R^3\cup\cdots)=I_A\cup R\cup R^2\cup R^3\cup\cdots$.

【定理 2-20】 设 $R\subseteq A\times A$，

(1) $rs(R)=sr(R)$.

(2) $rt(R)=tr(R)$(可记 $R^*=tr(R)$).

(3) $st(R)\subseteq ts(R)$.

证 只证明 (3)，(1)和(2)留作练习.

(3) $st(R)=s(R\cup R^2\cup\cdots)=(R\cup R^2\cup\cdots)\cup(R\cup R^2\cup\cdots)^{-1}=(R\cup R^2\cup\cdots)\cup(R^{-1}\cup (R^2)^{-1}\cup\cdots)=(R\cup R^2\cup\cdots)\cup(R^{-1}\cup(R^{-1})^2\cup\cdots)=(R\cup R^{-1})\cup(R^2\cup(R^{-1})^2)\cup\cdots\subseteq (R\cup R^{-1})\cup(R\cup R^{-1})^2\cup\cdots=ts(R)$.

下面的例子说明，定理 2-20(3)中，不能把“$\subseteq$”改为“$=$”.

【例 2-46】 试举例说明 $st(R)\neq ts(R)$.

解 设 $A=\{a,b,c\}$，令 $R=\{(a,b),(b,c)\}$，则

$$st(R) = s(t(R)) = \{(a,b),(b,c),(a,c),(b,a),(c,b),(c,a)\}$$
$$ts(R) = t(s(R)) = \{(a,b),(b,c),(b,a),(c,b),(c,a),(a,c),(a,a),(b,b),(c,c)\}$$

显然，$st(R)\neq ts(R)$.

习　题　2.4

1. 设 $R\subseteq A\times A$，则 $s(R)=R\cup R^{-1}$.

2. 设 $A=\{a,b,c,d\}$，A 上的关系

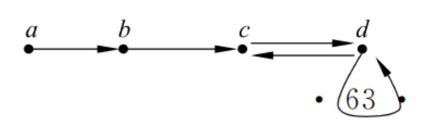


图　2-17

$$R=\{(a,a),(a,b),(b,a),(b,c),(c,d)\}$$

求 R 的自反闭包 $r(R)$、对称闭包 $s(R)$ 和传递闭包 $t(R)$.

3. 设关系 R 的关系图如图 2-17 所示，试分别给出 R 的自反闭包 $r(R)$、对称闭包 $s(R)$ 和传递闭包 $t(R)$ 的关系图.

4. 整数集合 $\mathbf{Z}$ 上的关系 $R=\{(x,y)|x,y\in\mathbf{Z}$ 且 $y=x+1\}$，试说明 R 的传递闭包 $t(R)$ 是小于关系“$<$”.

5. 设 R 和 S 是集合 A 上的关系，若 $R\subseteq S$，则下列结论均成立：

(1) $r(R)\subseteq r(S)$.

(2) $s(R)\subseteq s(S)$.

(3) $t(R)\subseteq t(S)$.

6. 设 $R_1\subseteq A\times A$，$R_2\subseteq A\times A$，则 $r(R_1\cup R_2)=r(R_1)\cup r(R_2)$.

7. 类似于定理 2-18，研讨关系的闭包运算与关系的交运算之间的联系.

8. 设 $R\subseteq A\times A$，若 R 自反，则 $s(R)$ 及 $t(R)$ 也自反.

9. 设 $R\subseteq A\times A$，

(1) 若 R 反自反，$s(R)$ 也反自反，但 $r(R)$ 和 $t(R)$ 不一定.

(2) 若 R 反对称，$r(R)$ 也反对称，但 $s(R)$ 和 $t(R)$ 不一定.

10. 设 $A=\{a,b,c\}$，$R=\{(a,b),(b,c)\}$，求 $rt(R)$.

11. 设 $R\subseteq A\times A$，证明

(1) $rs(R)=sr(R)$.

(2) $rt(R)=tr(R)$.

12. 设 $R\subseteq A\times A$，记 $R^+=t(R)$，$R^*=tr(R)$，证明：

(1) $(R^+)^+=R^+$；

(2) $(R^*)^*=R^*$；

(3) $R\circ R^*=R^*\circ R=R^+$.

2.5 等价关系

在实际应用时，具有某几种性质的关系是有用的. 接下来的 3 节内容，分别介绍集合 A 上的等价关系、相容关系和序关系.

等价关系是一种非常重要的特殊关系，它是相等关系“$=$”、全等关系“$\cong$”等的一种推广. 等价关系基于某种标准，如颜色相同、形状相同等，将不同的事物看成是同一类，又如研究整数时，基于能否被 2 整除观点将整数分为奇数和偶数两类进而有“奇数加偶数是奇数”的结论.

等价关系以及根据它对集合进行划分是**粗糙集**(rough set)理论的基础，粗糙集理论是智能信息处理的重要方法之一.

2.5.1 等价关系的定义

【定义 2-17】 设 $R\subseteq A\times A$，若 R 具有自反性、对称性以及传递性，则称 R 为 A 上的**等价关系**(equivalent relation).

【例 2-47】 设 $A=\{a,b,c\}$，$R=\{(a,a),(b,b),(c,c),(b,c),(c,b)\}$，很容易验证 R 是

A 上的等价关系.

【例 2-48】 试验证整数集 $\mathbf{Z}$ 上的模 3 同余关系(见第 2.1 节例 2-3)

$$R=\{(x,y) \mid x,y\in\mathbf{Z} \text{ 且 } 3\mid(x-y)\}$$

是 $\mathbf{Z}$ 上的等价关系.

解 (1) 任意 $x\in\mathbf{Z}$,由于 $3\mid(x-x)$,所以有 $(x,x)\in R$,于是 R 具有自反性.

(2) 任意 $x,y\in\mathbf{Z}$,若 $(x,y)\in R$,则 $3\mid(x-y)$,显然有 $3\mid-(x-y)$,即 $3\mid(y-x)$,于是有 $(y,x)\in R$,因此,R 具有对称性.

(3) 任意 $x,y,z\in\mathbf{Z}$,若 $(x,y)\in R$ 且 $(y,z)\in R$,则 $3\mid(x-y)$ 且 $3\mid(y-z)$,从而 $3\mid[(x-y)+(y-z)]$,即 $3\mid(x-z)$,所以 $(x,z)\in R$,因此,R 具有传递性.

根据定义知,R 是 $\mathbf{Z}$ 上的等价关系.

由 1.6 节定理 1-27 知,集合之间的对等关系"~"是等价关系.很容易证明:

【定理 2-21】 设 R 和 S 是集合 A 上的两个等价关系,则 R^{-1} 和 $R\cap S$ 是集合 A 上的等价关系.

证 根据等价关系的定义,由 2.3 节表 2-2 知结论成立.

设 R 和 S 是集合 A 上的两个等价关系,如表 2-4 所示为等价关系与关系运算的联系.

表 2-4

$R\cup S$	$R\cap S$	$\bar{R}$	$R-S$	$R\oplus S$	R^{-1}	$R\circ S$
×	√	×	×	×	√	×

2.5.2 等价类

【定义 2-18】 设 R 是 A 上的等价关系,对于任意 $a\in A$,称集合

$$\{x\mid x\in A \text{ 且 } (a,x)\in R\}$$

为元素 a 关于等价关系 R 所在的**等价类**(equivalent class),记为 $[a]_R$.

【例 2-49】 根据例 2-47 中的等价关系,求出 A 中各元素所在的等价类.

解 $[a]_R=\{a\}$,$[b]_R=\{b,c\}$,$[c]_R=\{b,c\}$.

虽然根据给定的等价关系,每个元素都有所在的等价类,但从例 2-49 可知,不同的等价类为 $\{a\}$,$\{b,c\}$.对于等价类 $\{b,c\}$,其代表元可以是 b:$[b]_R=\{b,c\}$,也可以是 c:$[c]_R=\{b,c\}$.根据定义,可以证明:

【定理 2-22】 设 R 是集合 A 上的等价关系,$x,y\in A$,则 $[x]_R=[y]_R$ 当且仅当 $(x,y)\in R$.

证 $(\Rightarrow)$ 因为 $(y,y)\in R$,所以根据等价类的定义有 $y\in[y]_R$.由已知 $[x]_R=[y]_R$,可得出 $y\in[x]_R$,所以有 $(x,y)\in R$.

$(\Leftarrow)$ 对于任意 $z\in[x]_R$,由定义有 $(x,z)\in R$.因为 $(x,y)\in R$,而 R 是等价关系,所以 $(y,x)\in R$,进而 $(y,z)\in R$.于是有 $z\in[y]_R$,因此有 $[x]_R\subseteq[y]_R$.同理可证 $[y]_R\subseteq[x]_R$,所以有 $[x]_R=[y]_R$.

【例 2-50】 根据例 2-48 中的等价关系,求出 $\mathbf{Z}$ 中各元素所在的等价类.

解 $\mathbf{Z}$ 中各元素所在的等价类分别为:

$[0]_R=\{\cdots,-6,-3,0,3,6,\cdots\}=\cdots=[-6]_R=[-3]_R=[0]_R=[3]_R=[6]_R=\cdots$

$[1]_R=\{\cdots,-5,-2,1,4,7,\cdots\}=\cdots=[-5]_R=[-2]_R=[1]_R=[4]_R=[7]_R=\cdots$

$[2]_R=\{\cdots,-4,-1,2,5,8,\cdots\}=\cdots=[-4]_R=[-1]_R=[2]_R=[5]_R=[8]_R=\cdots$

从上面两个例子还可以看出:不同的等价类是不相交的,即有下述定理.

【定理 2-23】 设 R 是集合 A 上的等价关系, $x,y\in A$, 若 $[x]_R\neq[y]_R$, 则 $[x]_R\cap[y]_R=\varnothing$.

证 (反证)若$[x]_R\cap[y]_R\neq\varnothing$,则存在 $z\in[x]_R\cap[y]_R$,于是$(x,z)\in R$ 且$(y,z)\in R$,进而$(z,y)\in R$,所以有$(x,y)\in R$.由定理 2-22,$[x]_R=[y]_R$,与已知矛盾.

【定义 2-19】 设 R 是集合 A 上的等价关系,称所有等价类组成的集合$\{[x]_R\mid x\in A\}$为集合 A 关于等价关系 R 的**商集**(quotient set),记为 A/R(读作 A 模 R),即

$$A/R=\{[x]_R\mid x\in A\}.$$

由例 2-49 知 $A/R=\{\{a\},\{b,c\}\}$,由例 2-50 知

$$\mathbf{Z}/R=\{\{\cdots,-6,-3,0,3,6,\cdots\},\{\cdots,-5,-2,1,4,\cdots\},\{\cdots,-4,-1,2,5,\cdots\}\}$$

它们分别是集合 $A=\{a,b,c\}$和整数集合 $\mathbf{Z}$ 的划分.

【定理 2-24】 设 R 是集合 A 上的等价关系,则 A 关于 R 的商集 A/R 是集合 A 的划分.

证 很容易证明等价关系的下列性质(留作练习):

(1) 每一个等价类$[x]_R$ 非空;

(2) 不同的等价类不相交(定理 2-23);

(3) 所有等价类的并是整个集合 A: $\bigcup_{x\in A}[x]_R=A$.

因此,给定集合 A 上的一个等价关系 R,根据该等价关系可以得到集合 A 的一种划分.反过来,若给定了集合 A 的一种划分 π,可以证明(留作练习)按下面的方式可构造出集合 A 上的一个**与划分 π 对应的等价关系 R**:

$$xRy\Leftrightarrow x \text{ 和 } y \text{ 在划分 } \pi \text{ 的同一个块中}.$$

【例 2-51】 设 $A=\{a,b,c\}$,A 上的划分 $\pi=\{\{a\},\{b,c\}\}$,试确定由 π 所产生的等价关系 R.

解 $R=\{(a,a),(b,b),(c,c),(b,c),(c,b)\}$.

我们知道,集合 $A=\{a,b,c\}$上的不同的划分共 5 个,通过计算知道集合 A 上的所有不同的等价关系也是 5 个,分别为:$R_1=A\times A$,$R_2=\{(a,b),(b,a)\}\cup I_A$,$R_3=\{(b,c),(c,b)\}\cup I_A$,$R_4=\{(a,c),(c,a)\}\cup I_A$,$R_5=I_A$.

可以证明:

【定理 2-25】 对于任意集合 A,集合 A 上的所有划分组成的集合 X 与其上的所有等价关系组成的集合 Y 是对等的.

证 对于任意给定的 $\pi\in X$,定义集合 A 上的等价关系 R 为 $xRy\Leftrightarrow x$ 和 y 在划分 π 的同一个块中.显然有 $A/R=\pi$.

按如下方式建立集合 X 到集合 Y 的映射 $f:\pi\rightarrow R$.

(1) 对于任意 $\pi_1,\pi_2\in X$,令 $f(\pi_1)=R_1$,$f(\pi_2)=R_2$,若 $f(\pi_1)=f(\pi_2)$,即 $R_1=R_2$,则 $A/R_1=A/R_2$,所以有 $\pi_1=\pi_2$,进而 f 是单射.

(2) 任意 $R\in Y$，由定理 2-24 知 $A/R\in X$. 显然，由划分 A/R 定义的等价关系就是 R，即存在 $\pi=A/R\in X$，使得 $f(\pi)=R$，所以 f 是满射.

故 f 是集合 X 到集合 Y 的一一对应. 证毕.

一种特殊的情况是 $A=\varnothing$，这时 $X=\varnothing$ 且 $Y=\varnothing$.

设 R_1 和 R_2 是集合 A 上的等价关系，由定理 2-21 知 $R_1\cap R_2$ 也是等价关系，这时 $A/(R_1\cap R_2)$ 与 A/R_1 和 A/R_2 之间的联系值得进一步研究(留作练习).

习　题　2.5

1. 设 $A=\{a,b,c,d\}$，验证 $R=\{(a,b),(b,a)\}\cup I_A$ 是 A 上的等价关系.

2. 设 $A=\mathbf{Z}\times\mathbf{Z}$，$A$ 上的关系 R 定义如下：

$$(x,y)R(u,v) \text{ 当且仅当 } x+v=y+u$$

证明 R 是 A 上的等价关系.

3. 设 R 和 S 分别是集合 A 和集合 B 上的等价关系，令

$$T=\{((x_1,y_1),(x_2,y_2))\mid (x_1,x_2)\in R,(y_1,y_2)\in S\}$$

证明：T 是 $A\times B$ 上的等价关系.

4. 对于正整数 k，验证整数集 $\mathbf{Z}$ 上的模 k 同余关系 $\equiv_k$：

$$x\equiv_k y \text{ 当且仅当 } k\mid(x-y)$$

是 $\mathbf{Z}$ 上的等价关系.

5. 设 X 是集合，$A=P(X)$，分别判断下述给定的 A 上的关系 R 是否是等价关系，说明理由.

(1) $R=\{(x,y)\mid x,y\in P(X)\text{且 } x\subseteq y \text{ 或 } y\subseteq x\}$.

(2) $R=\{(x,y)\mid x,y\in P(X)\text{且 } x\oplus y\subseteq C\}$，其中 $C\subseteq X$.

6. 设 R 和 S 是集合 A 上的两个等价关系，试举例说明下列各式不一定是集合 A 上的等价关系.

(1) $R\cup S$.

(2) $R-S$.

(3) $R\circ S$.

7. 设 $R\subseteq A\times A$，求出最小的包含 R 的等价关系.

8. 设 $A=\{a,b,c,d\}$，$R=\{(a,c),(c,a),(b,d),(d,b)\}\cup I_A$，

(1) 验证 R 是 A 上的等价关系.

(2) 求出商集 A/R.

9. 设 $f:A\to B$，定义 A 上的关系 R 如下：

$$R=\{(x,y)\mid x,y\in A,f(x)=f(y)\}$$

证明 R 是 A 上的等价关系.

10. 设 R 是集合 A 上的等价关系，则 A 关于 R 的商集 A/R 是集合 A 的划分.

11. 若给定了集合 A 的一种划分 π，证明按下面的方式构造出的集合 A 上的关系 R：

$$xRy \text{ 当且仅当 } x \text{ 与 } y \text{ 在划分 } \pi \text{ 的同一个块中}$$

是等价关系且商集 $A/R=\pi$.

12. 若$|A|=4$,求出 A 上所有的等价关系的个数.

13. 设 R_1 和 R_2 是集合 A 上的等价关系,考察 $A/(R_1\cap R_2)$与 A/R_1 和 A/R_2 的关系.

14. 设 R_1 和 R_2 是集合 A 上的等价关系,则对于集合 A 的划分,A/R_1 是 A/R_2 的加细划分当且仅当 $R_1\subseteq R_2$.

15. 设 R 是集合 A 上的等价关系,令

$$S=\{(x,y)\mid \exists c\in A,使(x,c)\in R 且(c,y)\in R\}$$

证明:S 是集合 A 上的等价关系.

16. 设 R 是集合 A 上的关系,构造 A 上的关系 S 如下:对于任意 $x,y\in A$,

$$(x,y)\in S\Leftrightarrow(x,y)\in R 且(y,x)\in R$$

要使得 S 是等价关系,关系 R 必须满足哪些性质?

2.6 相容关系

在实际问题中,两个事物具有某种共同的性质,如两个英文单词有一些相同字母、两个图形有些相似等,但与等价关系不同的是这种共性可能不具有传递性.

【例 2-52】 设集合 A 是由一些英文单词组成的 $A=\{\text{set},\text{logic},\text{algebra},\text{graph}\}$,考虑 $R=\{(x,y)|x,y\in A$ 且 x 与 y 有相同的字母$\}$,试验证 R 具有自反性和对称性,但不具有传递性.

解 对于任意 $x\in A$,显然 x 与 x 有相同的字母,即$(x,x)\in R$,于是 R 具有自反性.

对于任意 $x,y\in A$,若$(x,y)\in R$,则 x 与 y 有相同的字母,当然 y 与 x 有相同的字母,所以有$(y,x)\in R$,因此 R 具有对称性.

因为$(\text{set},\text{algebra})\in R$ 且$(\text{algebra},\text{graph})\in R$,但$(\text{set},\text{graph})\notin R$,所以 R 不具有传递性.

相容关系就是对具有这种性质的事物进行的数学描述,根据它可以得出集合的覆盖.

2.6.1 相容关系的定义

【定义 2-20】 设 $R\subseteq A\times A$,若 R 具有自反性和对称性,则称 R 为 A 上的**相容关系**(compatible relation)或**相似关系**(similar relation).

在实际问题中,相容有相似、相像或类似之意.显然,等价关系是相容关系,但相容关系不一定是等价关系,例 2-52 就是这方面的例子.容易验证,相容关系的传递闭包是等价关系.

【例 2-53】 设 $R\subseteq A\times A$,则 $R\cup R^{-1}\cup I_A$ 是集合 A 上的相容关系.

证 因为 $I_A\subseteq R\cup R^{-1}\cup I_A$,所以 $R\cup R^{-1}\cup I_A$ 是自反的.而$(R\cup R^{-1}\cup I_A)^{-1}=R^{-1}\cup(R^{-1})^{-1}\cup(I_A)^{-1}=R^{-1}\cup R\cup I_A=R\cup R^{-1}\cup I_A$,于是 $R\cup R^{-1}\cup I_A$ 是对称的.由此可知,$R\cup R^{-1}\cup I_A$ 是 A 上的相容关系.

【例 2-54】 设 R 和 S 是集合 A 上的两个相容关系,举例说明 $R\circ S$ 不必是 A 上的相容关系.

解 例如 $A=\{a,b,c\}$,取 $R=\{(a,b),(b,a)\}\cup I_A$,$S=\{(b,c),(c,b)\}\cup I_A$.显然 R 和 S 是集合 A 上的两个相容关系,但 $R\circ S=\{(a,c),(a,b),(b,a),(b,c),(c,b)\}\cup I_A$,这时$(a,c)\in R\circ S$,而$(c,a)\notin R\circ S$,于是 $R\circ S$ 不对称,进而 $R\circ S$ 不是 A 上的相容关系.

设 R 和 S 是集合 A 上的两个相容关系,表 2-5 列出了相容关系与关系运算的联系.

表 2-5

$R\cup S$	$R\cap S$	$\bar{R}$	$R-S$	$R\oplus S$	R^{-1}	$R\circ S$
√	√	×	×	×	√	×

在2.5节知道,由集合A的划分可得出集合A的等价关系,同样,根据集合A的覆盖可产生集合A的相容关系.先看一个例子.

【例 2-55】 设$A=\{a,b,c,d\}$,$\{A_1,A_2\}$是集合A的覆盖,其中$A_1=\{a,b,c\}$,$A_2=\{c,d\}$,这时

$$A_1\times A_1=\{(a,a),(a,b),(a,c),(b,a),(b,b),(b,c),(c,a),(c,b),(c,c)\}$$
$$A_2\times A_2=\{(c,c),(c,d),(d,c),(d,d)\}$$

令$R=(A_1\times A_1)\cup(A_2\times A_2)$,容易知道$R$是$A$上的相容关系.

一般地有以下定理:

【定理 2-26】 设$\{A_i|i\in I\}$是集合A的覆盖,则$R=\bigcup\limits_{i\in I}A_i\times A_i$是$A$上的相容关系.

证 (留作练习).

注意 集合A的不同覆盖按上面的方式可以得到集合A上的相同的相容关系.

【例 2-56】 设$A=\{a,b,c,d\}$,取集合A的覆盖为$\{\{a,b\},\{b,c\},\{a,c\},\{c,d\}\}$,则其产生的覆盖与例2-55中的覆盖$R$所产生的相容关系是相同的.

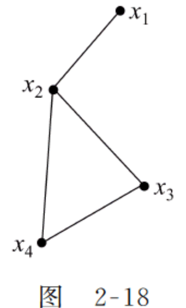


图 2-18

在例2-52中,令$x_1=\text{set}$,$x_2=\text{algebra}$,$x_3=\text{logic}$及$x_4=\text{graph}$,则$A=\{x_1,x_2,x_3,x_4\}$且$R=\{(x_1,x_2),(x_2,x_1),(x_2,x_3),(x_3,x_2),(x_2,x_4),(x_4,x_2),(x_3,x_4),(x_4,x_3)\}\cup I_A$.

在关系R的关系图G_R中,在任何点处都有环且任意两个不同的点之间若有边则成对出现.鉴于此,我们约定(1)每个点处的环省略;(2)成对出现的有向边用一条无向边代替,这样画出的图称为**相容关系R的简化关系图**.例2-52中的相容关系的简化关系图如图2-18所示.

2.6.2 相容类

由于一般的相容关系不是传递的,因此相容类的定义不同于等价类.

【定义 2-21】 设R是集合A上的相容关系,$\varnothing\neq C\subseteq A$,若对于任意$x,y\in C$,均有$(x,y)\in R$,则称$C$是由相容关系$R$产生的**相容类**(compatible class).

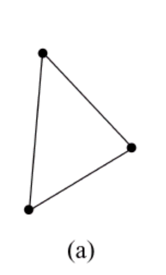
在例2-52中,$\{x_1\}$,$\{x_1,x_2\}$,$\{x_2\}$,$\{x_2,x_3\}$,$\{x_2,x_4\}$,$\{x_2,x_3,x_4\}$等是由相容关系R产生的相容类,而$\{x_1,x_3\}$等不是.

由相容关系R产生的相容类是很多的,我们主要关心的是极大相容类.

【定义 2-22】 设R是集合A上的相容关系,C是由相容关系R产生的相容类,若对于任意$C\subset D\subseteq A$,D不是相容类,则称C是由相容关系R产生的**极大相容类**(maximal compatible class).

可以证明,集合A中的任意元素至少在由相容关系R产生的一个极大相容类中.

在例2-52中,$\{x_1,x_2\}$,$\{x_2,x_3,x_4\}$是由相容关系R产生的所有的极大相容类.


(a)

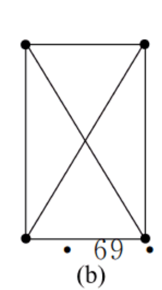

(b)

图 2-19

在相容关系 R 的简化关系图中,一个极大的完全多边形对应的 A 中元素构成一个极大相容类.所谓完全多边形是指该多边形的任意两个顶点都有边.特别地,一个点和一条线段是退化的完全多边形.如图 2-19 所示列举的分别是完全三边形和完全四边形.

由于集合 A 中的任意元素至少在由相容关系 R 产生的一个极大相容类中,所以所有的极大相容类构成集合 A 的一种覆盖.

习 题 2.6

1. 设集 A 是英文单词组成的 $A=\{$set, function, operation, relation, logic, algebra, graph$\}$,

$$R=\{(x,y)\mid x,y\in A \text{ 且 } x \text{ 与 } y \text{ 有相同的字母}\}$$

(1) 验证 R 是 A 上的相容关系.

(2) 试求出 R 中的所有元素.

(3) 画出相容关系 R 的简化关系图.

(4) 计算 R 产生的所有极大相容类.

2. 设 $A=\{1,2,3,4,5\}$, $R=\{(x,y)|x,y\in A,y=x+3\}$.

(1) 计算相容关系 $R\cup R^{-1}\cup I_A$.

(2) 求出 A 关于 $R\cup R^{-1}\cup I_A$ 的所有极大相容类.

3. 设$\{A_i|i\in I\}$是集合 A 的覆盖,则

(1) $R=\bigcup\limits_{i\in I}A_i\times A_i$是 A 上的相容关系.

(2) 说明在什么条件下,R 是等价关系.

4. 设 R 是集合 A 上的相容关系,则 $\bigcup\limits_{i=1}^{\infty}R^i$是 A 上的等价关系.

5. 设 R 和 S 为 A 上的相容关系,对于表 2-5 中的每一项,若是正确的给出证明,若是错误的举出反例.

2.7 偏序关系

在解决实际问题时,我们常依据某个标准对事物进行比较,同时按这个标准对两个事物之间的先后进行排序.在计算机科学中,对数据进行拓扑排序是十分有意义的工作[12].

偏序关系是最基本、最常用的一种序关系,它本质上是两实数之间的小于等于关系"$\leqslant$"的一种推广.

本节在偏序的基础上,介绍偏序集中的特殊元素.

2.7.1 偏序关系的定义

【定义 2-23】 设 $R\subseteq A\times A$,若 R 具有自反性、反对称性和传递性,则称 R 为 A 上的偏序关系,简称**偏序**(partial order).

先看两个在 2.3 节讨论过的例子.

【例 2-57】 证明:实数集 $\mathbf{R}$ 上的小于等于关系"$\leqslant$"是偏序关系.

证 (1) 对于任意 $x\in \mathbf{R}$,因为 $x\leqslant x$,所以$\leqslant$是自反的.

(2) 对于任意 $x,y\in \mathbf{R}$,若 $x\leqslant y$ 且 $y\leqslant x$,则必有 $x=y$,所以$\leqslant$是反对称的.

(3) 对于任意 $x,y,z\in \mathbf{R}$,若 $x\leqslant y$ 且 $y\leqslant z$,则有 $x\leqslant z$,所以$\leqslant$是传递的.

因此,$\leqslant$是实数集 $\mathbf{R}$ 上的偏序.

显然,自然数集 $\mathbf{N}$ 上或有理数集 $\mathbf{Q}$ 上的小于等于关系$\leqslant$也是其上的偏序关系.

【例 2-58】 证明:集合 X 的幂集 $P(X)$上的包含关系“$\subseteq$”是偏序关系.

证 (1) 对于任意 $A\in P(X)$,因为 $A\subseteq A$,所以$\subseteq$是自反的.

(2) 对于任意 $A,B\in P(X)$,若 $A\subseteq B$ 且 $B\subseteq A$,则必有 $A=B$,所以$\subseteq$是反对称的.

(3) 对于任意 $A,B,C\in P(X)$,若 $A\subseteq B$ 且 $B\subseteq C$,则有 $A\subseteq C$,所以$\subseteq$是传递的.

因此,$\subseteq$是 $P(X)$上的偏序.

由上面的两个例子可知,偏序关系是实数集合 $\mathbf{R}$ 上的小于等于关系“$\leqslant$”的一种推广.为了方便,对于一般的偏序 R 可记为“$\leqslant$”, 且称$(A,\leqslant)$为**偏序集**(partially ordered set, poset).之所以借用“$\leqslant$”这个符号,是因为一般的偏序 R 与小于等于关系“$\leqslant$”有类似的性质,且借助于小于等于关系“$\leqslant$”可以帮助理解偏序 R 的有关概念,如后面要讲的偏序集中的特殊元素.也正因为如此,一般的偏序“$\leqslant$”可以读作“小于等于”.

但要注意,一般意义上的偏序“$\leqslant$”与实数间的小于等于关系“$\leqslant$”在概念上是有一定区别的.考虑到这些区别,有些文献采用类似于小于等于关系$\preccurlyeq$(参见参考文献[8]).但对于特殊的偏序还是用大家熟悉的符号,如例 2-58 中的“$\subseteq$”以及下例中的偏序“$|$”.

【例 2-59】 证明:正整数集合 $\mathbf{N}^+$ 上的整除关系“$|$”是其上的偏序关系.

证 (1) 对于任意 $x\in \mathbf{N}^+$,因为 $x|x$,所以$|$是自反的.

(2) 对于任意 $x,y\in \mathbf{N}^+$,若 $x|y$ 且 $y|x$,则必有 $x=y$,所以$|$是反对称的.

(3) 对于任意 $x,y,z\in \mathbf{N}^+$,若 $x|y$ 且 $y|z$,则有 $x|z$,所以$|$是传递的.

因此,$|$ 是正整数集合 $\mathbf{N}^+$ 上的偏序.

但要注意,整数集合 $\mathbf{Z}$ 上的整除关系不是其上的偏序关系, 因为 $2|-2$ 且 $-2|2$, 但 $2\neq -2$, 即整数集合 $\mathbf{Z}$ 上的整除关系不具有反对称性.

线性序关系是最常见、最简单的一种偏序关系.

【定义 2-24】 设$(A,\leqslant)$是偏序集,若对任意 $x,y\in A$,有 $x\leqslant y$ 或 $y\leqslant x$,则称$\leqslant$是线性序关系,简称**线性序**(linear order),又称为**全序**(total order).

显然,实数集上的数的小于等于关系$\leqslant$是线性序.

【例 2-60】 设 $R\subseteq A\times A$,若 R 具有反自反性和传递性,则称 R 为 A 上的拟序关系,简称**拟序**(quasi-order).证明

(1) 拟序具有反对称性.

(2) 若 R 为 A 上的拟序,则 $r(R)=R\cup I_A$ 为 A 上的偏序.

(3) 若 R 为 A 上的偏序,则 $R-I_A$ 为 A 上的拟序.

证 (1) 对于任意 $x,y\in A$,若$(x,y)\in R$ 且$(y,x)\in R$,因为 R 传递,所以有$(x,x)\in R$,与 R 反自反矛盾,因此$(x,y)\in R$ 与$(y,x)\in R$ 不能同时成立,故拟序具有反对称性.

(2)(3)(留作练习).

几种满足特殊性质的关系如表 2-6 所示.

表 2-6

关系＼性质	自反	反自反	对称	反对称	传递
等价关系	✓	×	✓	×	✓
相容关系	✓	×	✓	×	×
偏序	✓	×	×	✓	✓
拟序	×	✓	×	✓	✓

2.7.2 偏序集的哈斯图

在偏序的关系图中，每个点处都有环，可以不必画出来. 又因为它的反对称性和传递性，其边的方向是一致的，比如都是从下到上方向，更主要的是可去掉由于传递出现的边，同时去掉边的方向. 按这种方式得到的图就是**哈斯图**(Hasse diagram)，是以德国数学家 Helmut Hasse 的名字命名的.

【例 2-61】 设 $A=\{1,2,3,4\}$，A 上的数的小于等于关系≤是其上的偏序关系，试画出 $(A,\leqslant)$ 的哈斯图.

解 A 关于≤的关系图见图 2-20(a)，哈斯图见图 2-20(b).

显然，哈斯图表明了偏序集中的元素按相对大小、位置进行的排序.

(a) (b)

图 2-20

为了更具体说明哈斯图的画法，先定义偏序集中元素 y 盖住元素 x.

【定义 2-25】 设 $(A,\leqslant)$ 是偏序集，$x,y\in A$，若下列三个条件同时成立，则称**元素 y 盖住元素 x**：

(1) $x\neq y$.

(2) $x\leqslant y$.

(3) 不存在异于 x 和 y 的元素 $z\in A$，使 $x\leqslant z$ 且 $z\leqslant y$ 同时成立.

直观地看，y 盖住 x 是指 y 是 x 的“顶头上司”. 记 $\mathrm{COV}(A)=\{(x,y)\mid x,y\in A$ 且 y 盖住 $x\}$.

【例 2-62】 设 $X=\{a,b\}$，令 $A=P(X)=\{\varnothing,\{a\},\{b\},\{a,b\}\}$，集 A 上的包含关系“$\subseteq$”是其上的偏序关系，求 $\mathrm{COV}(A)$.

解 根据定义知，$\{a\}$ 盖住 $\varnothing$，$\{b\}$ 盖住 $\varnothing$，$\{a,b\}$ 盖住 $\{a\}$，$\{a,b\}$ 盖住 $\{b\}$. 因此 $\mathrm{COV}(A)=\{(\varnothing,\{a\}),(\varnothing,\{b\}),(\{a\},\{a,b\}),(\{b\},\{a,b\})\}$.

设 $(A,\leqslant)$ 是偏序集，按下面方式画出的图称为 $(A,\leqslant)$ 的哈斯图：

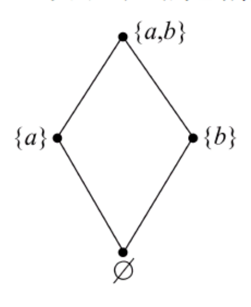


图 2-21

(1) 用黑点或小圆圈代表集合 A 中的元素.

(2) 对于任意 $(x,y)\in\mathrm{COV}(A)$，即 y 盖住 x，都将 y 画在 x 的上方且在 y 与 x 之间画一条无向边.

注意 只有一条线上的两个元素可以比较大小：下方元素≤上方元素，不同线上的两个元素不能比较大小，即没有关系，这是偏序名称的来历. 线性序的哈斯图是一条链(chain).

例 2-62 中的偏序集的哈斯图见图 2-21. $(P(\{a,b,c\}),\subseteq)$ 的哈斯

图见图 5-4(c).

2.7.3 偏序集中的特殊元素

在偏序集$(A,\leqslant)$中,设$\varnothing\neq S\subseteq A$,对于$A$中的偏序$\leqslant$而言,$S$中处于某些特殊位置的元素是很重要的.建议在理解这些特殊元素时,将偏序$\leqslant$当作“小于等于”,虽然它一般不是数的小于等于.

【定义 2-26】 设$(A,\leqslant)$是偏序集,$\varnothing\neq S\subseteq A$,$b\in S$.

(1) 若对于任意$x\in S$,均有$x\leqslant b$,则称b是子集S的**最大元**(greatest element).

(2) 若对于任意$x\in S$,均有$b\leqslant x$,则称b是子集S的**最小元**(least element).

例 2-57 中的偏序集$(\mathbf{R},\leqslant)$中,若取$S=\mathbf{Z}$,则S既无最大元也无最小元,这就说明一个子集的最大(小)元不一定存在.

在例 2-58 中的$(P(X),\subseteq)$中,取$S=P(X)$,因为对于任意$A\in P(X)$,均有$A\subseteq X$,所以S的最大元是X.同理可知,S的最小元是$\varnothing$.

就整除关系而言,因为对于任意$x\in\mathbf{N}^+$,均有$1|x$,于是例 2-59 中的偏序集中,$\mathbf{N}^+$的最小元是 1.因为没有被所有正整数整除的正整数,所以$\mathbf{N}^+$无最大元.

若取$S=\{2,4,6,12\}$,则S的最大元为 12, S的最小元为 2.

【定理 2-27】 在偏序集$(A,\leqslant)$中,$\varnothing\neq S\subseteq A$,若$S$的最大(小)元存在,则是唯一的.

证 设a, b是S的最大元, 因为a是最大元,所以有$b\leqslant a$;同样,因为b是最大元,所以有$a\leqslant b$.由于偏序$\leqslant$是反对称的,因而有$a=b$.同理可证最小元的唯一性.

在偏序集$(A,\leqslant)$中,A的最大元通常记为 1, A的最小元通常记为 0.

借助于偏序集合$(A,\leqslant)$中非空集合S的最小元的概念,可以给出以下定义:

【定义 2-27】 设$(A,\leqslant)$是偏序集,若对于任意$\varnothing\neq S\subseteq A$,$S$都存在最小元,则称$\leqslant$是$A$上的**良序**(well order),称$(A,\leqslant)$是**良序集**(well ordered set).

【例 2-63】 证明:自然数集合$\mathbf{N}$关于数的小于等于关系$\leqslant$是良序集.

证 对于任意$\mathbf{N}$的非空子集合S,在S中取一个元素,再判断比它小的元素是否属于S即可得出S的最小元,故$(\mathbf{N},\leqslant)$是良序集.

可以证明以下定理.

【定理 2-28】 任意良序集$(A,\leqslant)$是线性序集.

证 对于任意$x,y\in A$,由于$(A,\leqslant)$是良序集,所以$\{x,y\}$必存在最小元,比如说x,显然$x\leqslant y$,即$(A,\leqslant)$是线性序集.

一般来说,线性序不一定是良序.

【例 2-64】 验证:$(\mathbf{Z},\leqslant)$是线性序,但不是良序.

解 显然,$(\mathbf{Z},\leqslant)$是线性序.由于$\mathbf{Z}$本身就不存在最小元,所以$(\mathbf{Z},\leqslant)$不是良序集合.

容易证明以下定理.

【定理 2-29】 任意有限的线性序集合是良序集合.

下面继续讨论偏序集合中的另外一些特殊元素.

【定义 2-28】 设$(A,\leqslant)$是偏序集,$\varnothing\neq S\subseteq A$,$b\in S$.

(1) 对于任意$x\in S$,若$b\leqslant x$,有$x=b$,则称b是子集S的**极大元**(maximal element).

（2）对于任意 $x\in S$，若 $x\leqslant b$，有 $x=b$，则称 b 是子集 S 的**极小元**(minimal element).

事实上，b 是 S 的极大元是指 S 中没有比 b 更大的元素；b 是 S 的极小元是指 S 中没有比 b 更小的元素.

在例 2-57 中，取 $S=\mathbf{R}$，则 S 既无极大元也无极小元，这就说明子集的极大(小)元不一定存在.

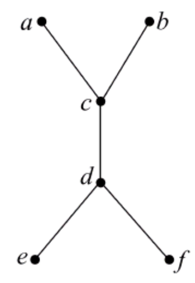


图 2-22

【例 2-65】 哈斯图(如图 2-22 所示)的偏序集中，$\{a,b,c,d,e,f\}$的极大元是 a，b；$\{a,b,c,d,e,f\}$的极小元是 e，f.

上述例子说明，一个子集的极大(小)元不一定存在. 若存在也不一定唯一. 但若 S 的最大(小)元存在，则 S 的极大(小)元存在且唯一.

显然，在偏序集 $(A,\leqslant)$ 中，任意有限的非空子集都存在极小元. 若 A 是有限集，利用这个结论可以在集合 A 上定义一个与$\leqslant$一致的线性序，进而将 A 进行拓扑排序，其算法参见参考文献[2].

【定义 2-29】 设$(A,\leqslant)$是偏序集，$\varnothing\neq S\subseteq A$.

（1）若存在 $a\in A$，对于任意 $x\in S$，均有 $x\leqslant a$，则称 a 为子集 S 的**上界**(upper bound).

（2）若存在 $a\in A$，对于任意 $x\in S$，均有 $a\leqslant x$，则称 a 为子集 S 的**下界**(lower bound).

容易知道，A 中元素 a 是 S 上(下)界是指 a 在 S 中每一个元素的上(下)方.

在例 2-65 中，取 $S=\{c,d\}$，则 S 的上界为 a，b，c，S 的下界为 d，e，f. 若取 $S=\{a,b,c,d,e,f\}$，则 S 既无上界也无下界，只需注意元素 a 和 b，以及元素 e 和 f 是没有偏序关系的.

【定义 2-30】 设$(A,\leqslant)$是偏序集，$\varnothing\neq S\subseteq A$.

（1）子集 S 的最小上界称为 S 的**上确界**(least upper bound)，记为 $\mathrm{lub}(S)$或 $\sup(S)$.

（2）子集 S 的最大下界称为 S 的**下确界**(greatest lower bound)，记为 $\mathrm{glb}(S)$或$\inf(S)$.

因为子集 S 的上(下)界不一定存在，所以子集 S 的上(下)确界不一定存在. 下例说明，即使子集 S 的上(下)界存在，子集 S 的上(下)确界也不一定存在.

【例 2-66】 在哈斯图如图 2-23 的偏序集中，试说明$\{d,e\}$有上界但无上确界，$\{b,c\}$有下界但没有下确界.

图 2-23

解 显然，a,b,c 是$\{d,e\}$的上界，但由于$\{a,b,c\}$无最小元，即$\{d,e\}$无上确界. 同样，d,e,f 是$\{b,c\}$的下界，而$\{d,e,f\}$无最大元，即$\{b,c\}$无下确界.

【定理 2-30】 设$(A,\leqslant)$是偏序集，$\varnothing\neq S\subseteq A$，若 S 的上(下)确界存在，则唯一.

证 (留作练习).

【例 2-67】 设 X 是集合，证明：偏序集$(P(X),\subseteq)$中任意两个元素均存在上确界以及下确界.

证 对于任意 $A,B\in P(X)$，显然 $A\cup B\in P(X)$. 由于 $A\subseteq A\cup B$ 且 $B\subseteq A\cup B$，所以 $A\cup B$ 是 A 和 B 的上界. 假设 C 是 A 和 B 的上界，即 $A\subseteq C$，$B\subseteq C$，因此 $A\cup B\subseteq C$，故 $A\cup B$ 是 A 和 B 的最小上界，即有 $\sup\{A, B\}=A\cup B$. 同理可证，$\inf\{A, B\}=A\cap B$.

【例 2-68】 设 $\mathbf{N}^+$ 是集合，证明：偏序集$(\mathbf{N}^+,|)$中任意两个元素均存在上确界以及下确界，其中$|$是整除关系.

证 对就整除关系而言，对于任意 $x,y\in\mathbf{N}^+$，令 x 与 y 的最小公倍数为 $\mathrm{lcm}(x, y)$，根据公倍数的定义知，$x|\mathrm{lcm}(x, y)$且 $y|\mathrm{lcm}(x, y)$，所以 $\mathrm{lcm}(x, y)$是$\{x,y\}$的上界. 假定 z 是$\{x,y\}$的上界，则 $x|z$ 且 $y|z$，即 z 是 x 与 y 的倍数，根据最小公倍数的定义知，$\mathrm{lcm}(x, y)|z$，于是 $\mathrm{lcm}(x, y)$是$\{x,y\}$的上确界. 同样可证，x 与 y 的最大公约数 $\gcd(x, y)$是$\{x,y\}$的下确界.

习 题 2.7

1. 令 D_{12}是 12 的所有正公因数组成的集合，证明其上的整除关系"$|$"是偏序关系，并画出$(D_{12},|)$的哈斯图.

2. 设集合 $A=\{a,b,c,d,e\}$上的关系为

$$R=\{(a,a),(a,b),(a,c),(a,d),(a,e),(b,b),(b,c),(b,e),(c,c),(c,e),(d,d),(d,e),(e,e)\}$$

证明：(A,R)是偏序集，并画出哈斯图.

3. 若$(A,\leqslant)$是偏序集，$S\subseteq A$，证明：$\leqslant$在 S 上的限制$\leqslant|_S$ 是 S 上的偏序. 通常将$(S,\leqslant|_S)$记为$(S,\leqslant)$.

4. 若$(A,\leqslant)$是偏序集，记$\leqslant^{-1}$为$\geqslant$，证明$(A,\geqslant)$是偏序集.

5. 设 R 和 S 是集合 A 上的两个偏序，表 2-7 列出了偏序与关系运算的联系.

表 2-7

$R\cup S$	$R\cap S$	$\bar{R}$	$R-S$	$R\oplus S$	R^{-1}	$R\circ S$
×	√	×	×	×	√	×

正确的给出证明，错误的给出反例.

6. 证明：(1) 若 R 为 A 上的拟序，则 $r(R)=R\cup I_A$ 为 A 上的偏序.

(2) 若 R 为 A 上的偏序，则 $R-I_A$ 为 A 上的拟序.

7. 证明：任意有限的非空偏序集$(A,\leqslant)$都存在极小元及极大元.

8. 设偏序集$(A,\leqslant)$的哈斯图如图 2-24 所示.

(1) 求集合 A 的最大元素、最小元素、极大元素和极小元素.

(2) 求子集$\{b,c,d\}$的上界、下界、上确界和下确界.

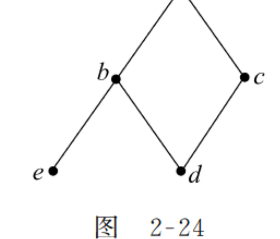


图 2-24

9. 设$(A,\leqslant)$是偏序集，$\varnothing\neq S\subseteq A$，若 S 的上(下)确界存在，则一定唯一.

10. 在偏序集$(P(X),\subseteq)$中，证明：$\inf\{A, B\}=A\cap B\in P(X)$.

11. 设 $F(\mathbf{N})$是自然数集合 $\mathbf{N}$ 的全体有限子集组成的集合.

(1) 证明：$(F(\mathbf{N}), \subseteq)$是偏序集.

(2) $(F(\mathbf{N}), \subseteq)$是否有极大元，为什么？

(3) $(F(\mathbf{N}), \subseteq)$是否有极小元,为什么?

(4) 对于任意 $A,B\in F(\mathbf{N})$,是否存在 $\sup\{A, B\}$?

(5) 对于任意 $A,B\in F(\mathbf{N})$,是否存在 $\inf\{A, B\}$?

12. 设 S 为集合且 $A=P(S)-\{S,\varnothing\}\neq\varnothing$,求$(A,\subseteq)$的极小元、极大元、最小元及最大元.

13. 设 A 和 B 是集合,$A\neq\varnothing$,$(B,\leqslant)$是偏序集.定义 B^A 上的关系 R 如下:

$$(f,g)\in R\Leftrightarrow f(x)\leqslant g(x),\quad \forall x\in A$$

(1) 证明:关系 R 是 B^A 上的偏序.

(2) 给出(B^A,R)存在最大元的必要条件和最大元的一般形式.

14. 设 A 是集合,P 是 A 的所有划分组成的集合,对于任意 $\pi_1\in P$ 和 $\pi_2\in P$,规定 P 上的关系 R 如下:

$$\pi_1 R\pi_2 \Leftrightarrow \forall X\in\pi_1, \exists Y\in\pi_2, X\subseteq Y$$

则 R 是集合 P 上的偏序.

本章小结

1. 关系的概念

离散数学研究离散对象，主要研究对象之间的联系,即关系. n 个对象之间的关系就是 n 元关系，借助于集合可对 n 元关系建立数学模型.

设 A 和 B 是集合，若 $R\subseteq A\times B$，则称 R 为 A 到 B 的 2 元关系. 集合 A 上的 2 元关系 R 是指 $R\subseteq A\times A$. 若$|A|=m$,$|B|=n$，则 A 与 B 间的关系共有 2^{mn} 个.

深入理解整数集 $\mathbf{Z}$ 上整除关系和模 m 同余关系，理解模 m 同余关系的性质和 3 个重要定理，能进行简单的同余线性方程和同余线性方程组的求解.

关系 R 中所有序偶第一坐标构成的集合为 R 的定义域 $\mathrm{dom}\,R$，所有序偶第二坐标构成的集合为 R 的值域 $\mathrm{ran}\,R$.

熟练 A 到 B 的关系和 A 上的关系的关系图表示方法，能写出关系的关系矩阵.

了解函数的关系定义. 实际上，关系是函数的推广.

2. 关系的运算

关系是集合，所以关系可进行集合运算 $R\cup S$,$R\cap S$,$\bar{R}$,$R-S$,$R\oplus S$.

设 $R\subseteq A\times B$,则

$$R^{-1}=\{(y,x)\mid(x,y)\in R\}.$$

设 A, B, C 是集合,若 $R\subseteq A\times B$,$S\subseteq B\times C$,则 $R\circ S=\{(x,z)|x\in A,z\in C$,存在 $y\in B$ 使得 $(x,y)\in R,(y,z)\in S\}$.

熟练掌握关系的运算及与运算有关的结论.

3. 关系的性质

关系的性质是本章重点内容之一，也是难点内容.

(1) 设 $R\subseteq A\times A$,若对于任意 $x\in A$,均有$(x,x)\in R$,则 R 就是 A 上的自反关系. R 在

A 上自反的充要条件是 $I_A \subseteq R$.

(2) 设 $R \subseteq A \times A$,若对于任意 $x \in A$,均有 $(x,x) \notin R$,则 R 就是 A 上的反自反关系. R 在 A 上反自反的充要条件是 $I_A \cap R = \varnothing$.

(3) 设 $R \subseteq A \times A$,对于任意 $x,y \in A$,如果 $(x,y) \in R$,那么有 $(y,x) \in R$,则 R 就是 A 上的对称关系. R 在 A 上对称的充要条件是 $R = R^{-1}$.

(4) 设 $R \subseteq A \times A$,对于任意 $x,y \in A$,如果 $(x,y) \in R$ 且 $(y,x) \in R$,那么一定有 $x = y$,则 R 就是 A 上的反对称关系. R 在 A 上反对称的充要条件是 $R \cap R^{-1} \subseteq I_A$.

(5) 设 $R \subseteq A \times A$,对于任意 $x,y,z \in A$,如果 $(x,y) \in R$ 且 $(y,z) \in R$,那么 $(x,z) \in R$,则 R 就是 A 上的传递关系. 关系 R 在 A 上传递的充要条件是 $R \circ R \subseteq R$.

4. 关系的闭包

设 $R \subseteq A \times A$,最小的包含 R 的自反(对称、传递)关系就是 R 的自反闭包 $r(R)$(对称闭包 $s(R)$、传递闭包 $t(R)$).

$$r(R) = R \cup I_A$$

$$s(R) = R \cup R^{-1}$$

$$t(R) = \bigcup_{i=1}^{\infty} R^i = R \cup R^2 \cup R^3 \cup \cdots$$

要求熟练掌握关系的闭包运算，能根据闭包的定义、关系图及上述计算公式求出关系的闭包(较少使用传递闭包公式进行计算).

5. 等价关系

设 $R \subseteq A \times A$，若 R 具有自反性、对称性以及传递性,则 R 就是 A 上的等价关系.

设 R 是 A 上的等价关系,对于任意 $a \in A$,元素 a 关于等价关系 R 所在的等价类

$$[a]_R = \{x \mid x \in A \text{ 且} (a,x) \in R\}$$

集合 A 的划分 π 与集合 A 上的等价关系 R 可以建立一一对应关系 $f:\pi \to R$. 实际上，集合 A 上等价关系 R 是划分集合 A 的标准. 要求掌握等价关系的定义及等价类的计算.

6. 相容关系

设 $R \subseteq A \times A$，若 R 具有自反性和对称性,则称 R 为 A 上的相容关系或相似关系. 设 $\{A_i \mid i \in I\}$ 是集合 A 的覆盖,则 $R = \bigcup_{i \in I} A_i \times A_i$ 是 A 上的相容关系.

理解相容关系的定义，了解相容类和极大相容类.

7. 偏序关系

设 $R \subseteq A \times A$,若 R 具有自反性、反对称性和传递性,则 R 就是 A 上的偏序. 设 $(A,\leqslant)$ 是偏序集,若对任意 $x,y \in A$,有 $x \leqslant y$ 或 $y \leqslant x$,则 $\leqslant$ 就是 A 上的线性序或全序.

设 $(A,\leqslant)$ 是偏序集，y 盖住 x 是指 y 是 x 的“顶头上司”. 哈斯图的画法：

(1) 用黑点或小圆圈代表集合 A 中的元素；

(2) 若 y 盖住 x,就将 y 画在 x 的上方且在 y 与 x 之间画一条线. 哈斯图表明了偏序集中的元素之间的层次结构.

除要求掌握偏序集的定义和哈斯图的画法外，还要会计算偏序集中满足要求的特殊元素.

设 $(A,\leqslant)$ 是偏序集,$\varnothing \neq S \subseteq A$：

（1）$b\in S$，S 中每个元素 x，$x\leqslant b$，b 就是 S 的最大元. $b\in S$，S 中每个元素 x，$b\leqslant x$，b 就是 S 的最小元.

（2）$b\in S$，若 S 中没有比 b 更大(小)的元素，b 就是 S 的极大(小)元.

（3）A 中元素 a 是 S 上(下)界是指 a 在 S 中每一个元素的上(下)方.

（4）S 的最小上界是 S 的上确界，S 的最大下界是 S 的下确界.

第3章　命题逻辑

逻辑是一个常用的术语，平时说话、做事、思考问题等都要合乎逻辑．比如，一位老师正在学校上课，而要说他在太空漫步就不合乎逻辑，把“逻辑地址”弄错了．同时，逻辑推理也无处不在，从日常生活中的实际问题的解决到数学定理的证明以及程序正确性验证．

逻辑学是研究思维形式、思维方法及思维规律尤其是推理的学科，早在两千多年前就受到人们的重视，古希腊著名逻辑学家亚里士多德（Aristotle，公元前 384—公元前 322）是形式逻辑的创始人．形式逻辑，现在称为普通逻辑学，要详细讨论概念（词项）、判断（命题）和各种形式的推理，研究逻辑基本规律等内容．

联合国教科文组织将逻辑学列为与数学、物理学、化学、天文学、地学、生物学同等重要的基础学科，在我国 MBA、MPA 以及工程硕士入学考试加入了逻辑测试题，国内很多大公司、企业招聘高级员工时也开始加试逻辑测试．

德国数学家、哲学家莱布尼茨（G. Leibniz，1647—1716）首先提出用数学方法研究逻辑，就是建立一套表意符号体系，在符号之间进行形式推理．莱布尼茨是数理逻辑的创始人．也正因为这样，数理逻辑又称为符号逻辑．

逻辑推理无处不在，从日常生活中的实际问题的解决到数学定理的证明以及程序正确性验证．

除了传统的数理逻辑（内容包括逻辑演算、公理化集合论[13]、模型论、递归论和证明论）外，还出现了各种各样的应用逻辑，如多值逻辑、模态逻辑、归纳逻辑、时序逻辑、动态逻辑、模糊逻辑、非单调逻辑、默认逻辑、数字逻辑、电路逻辑、算法逻辑及程序逻辑等，这些都与计算机科学密切相关，参考有关文献[14]．

人们需要学习、思考机器特别是计算机是如何进行逻辑思维的，以便用硬件或软件去模拟（广义下的计算）实现人的逻辑思维，这是一种最好的计算思维（computational thinking）培养形式．

命题逻辑与谓词逻辑是数理逻辑的基础部分．本章学习命题逻辑，内容涉及集合、映射、运算和关系等．

命题逻辑的研究对象是命题．

3.1　命题的有关概念

计算机的计算过程就是推理过程，而每一步推理离不开判断，判断的对象就是命题．

什么是命题？**命题**（proposition 或 statement）是能判断出真假（或真假程度）的语句．可以从三个方面去理解：

（1）命题必须是一个完整的句子，包括用数学式子如 $2+3=5$ 代表的语句．这一点在后面的命题符号化时要注意．

（2）所给语句具有真假意义，即有是否符合客观实际或是否合理之分．一般来说，只有

陈述句才可能具有真假意义，祈使句、疑问句和感叹句不具有真假意义.

(3) 能判断出真假. 不过，要是将来某时候能判断出真假也行.

【例 3-1】 判断下列语句是否是命题.

(1) 辽宁舰是中国的第一艘航空母舰.

(2) 我喜欢智能手机和平板电脑.

(3) $x>3$.

(4) 立正！

(5) 这朵花真漂亮！

(6) 你要我的手机号码是想给我充话费？

(7) 火星上有生物.

(8) 这句话是假话.

(9) 小王和小李是同学.

(10) 你只有刻苦学习，才能取得好成绩.

解 很显然，(1)和(2)是命题.

(3) 不是命题，因为无法知道变量 x 的取值，进而无法确定其真假.

(4) 是祈使句，它本身没有对错之分，但命令发出后会有终结反应.

(5) 是感叹句，(6)是疑问句，没有真假意义(反诘句如"你也喜欢《潜伏》吗？"除外). 不过，也可以认为(5)是"这朵花漂亮"的强调形式，因而是命题.

在 2005 年，美国"发现"号探测器发现火星上有水，至今尚不知道火星上是否有生物，2012 年着陆火星的"好奇"号正在探测，但我们相信在将来某个时候一定会知道的，因此，(7)被认为是命题. 正如我们把哥德巴赫(C. Goldbach, 1690—1764)1742 年猜想"1＋1＝2"，即"大于 4 的偶数是两个奇素数之和"看作命题一样，现已经对直到 10^{14} 的所有的大于 4 的偶数都已经验证结论是正确的. 1966 年我国数学家陈景润证明了"1＋2＝3"，即"一个充分大的偶数是一个奇素数和一个不超过两个奇素数乘积的数之和".

(8) 是悖论，不管承认对还是错都会导致矛盾. 若一个理论中出现悖论，说明该理论有不合理的地方. 为了避免悖论的出现，也许会产生新的研究分支，如公理化集合论等.

(9)和(10)是命题.

虽然，问题的重点不在于判断一个语句是否是命题，特别是命题的真假问题，因为有些判断还涉及概念的内涵问题，但对于初学用符号去研究逻辑的人来说，理解命题概念还是非常必要的.

命题的**真值**(truth)就是命题的逻辑取值. 经典逻辑值只有两个：1 和 0，它们是表示事物状态的两个量. 若一个命题是真命题，其真值为 1；若一个命题是假命题，其真值为 0. 在计算机专业课程中，将逻辑真用 1 表示，逻辑假用 0 表示. 通常规定，1 表示开关处于接通状态，0 表示开关处于断开状态；三极管饱和用 1 表示，三极管截止用 0 表示；在电路分析和设计时规定，1 表示高于逻辑高电平信号，0 表示逻辑低电平信号等. 实际上在数理逻辑中，更多时候逻辑真是用 T(True)，逻辑假用 F(False)表示的.

若一个命题不包含有更小的命题，则称其为**原子命题**(atom)或简单命题，否则称为**复合命题**(compound proposition). 原子命题是命题逻辑研究的基本单位，区分原子命题在后面命题的符号化时是很重要的. 在例 3-1 中，(1)、(2)、(7)、(9)是原子命题，特别注意(9)是

原子命题，不能把它分解为“小王是同学”和“小李是同学”.(10)是复合命题，它包含有两个原子命题“你刻苦学习”和“你取得好成绩”.

通常用小写英文字母 $p,q,r,s,\cdots$ 或带下标 $p_1,p_2,p_3,\cdots$ 等来表示原子命题，如用 p：$2+3=5$，q：今天我们上课.

现在已经向构造符号体系迈出了第一步.还有的联结词符号将在下节介绍.把 1 和 0 称为**逻辑常量**(logical constant)，今后在逻辑表达式中出现的 $p,q,r,s,\cdots$ 或 $p_1,p_2,p_3,\cdots$ 等称为**命题变元**(proposition variable)或**逻辑变量**(logical variable).命题变元可以代表任意命题，从取值的角度看，命题变元既可以取 1 也可以取 0.

习 题 3.1

1. 指出下列语句哪些是命题，对于命题指出其真值.

(1) 北京在 2008 年举办奥运会.

(2) 离散数学是计算机专业的必修课.

(3) $x>y$.

(4) 西南大学是一所“211 工程”建设的学校.

(5) 1 是素数.

(6) 读大学就是要学会思考.

(7) 月收入超过 3500 元要上缴个人所得税.

2. 找出下列各命题的所有原子命题，并分别用小写英文字母表示.

(1) 我不去游泳.

(2) 张三一边看书，一边用 iphone 听音乐.

(3) 小李能歌善舞.

(4) 这学期我选修“人工智能”或“模式识别”课程.

(5) 明天去深圳的飞机是上午八点或上午八点半起飞.

(6) 如果我有时间，我就回家去看望我的父母.

(7) 我今天进城，除非天下雨.

(8) 小张既没有外出也没有上网，他在睡觉.

(9) 你只有刻苦学习，才能取得好成绩.

(10) 仅当你走，我留下值班.

3.2 逻辑联结词

命题逻辑中出现的命题，除原子命题外，更多的是复合命题.一方面，复合命题是由原子命题构成的，它需要联结词；另一方面，给定了原子命题，使用**逻辑联结词**(logical connectives)可以将它们构成一个复合命题，这也是逻辑联结词的作用之一.

逻辑联结词类似于自然语言中的连词，但逻辑联结词就是逻辑运算，除在本节对其进行严格定义外，还需要在其后讨论其运算性质.

3.2.1 否定联结词 $\neg p$

设 p 表示一个命题，$\neg p$ 是对命题 p 的**否定**(negation，not)，读作“非 p”.

例如，令 p：$2+3=5$，则 $\neg p$：$2+3\neq 5$. 于是，1 元运算 $\neg$ 的运算表，如表 3-1 所示.

表 3-1

p	$\neg p$
1	0
0	1

$\neg p$ 也可以用 $\sim p$ 表示，在 C 语言中用 $!p$ 表示，在信息检索中用 $-p$ 表示，在数字逻辑以及计算机组成原理中用 $\bar{p}$ 表示，与其对应的门电路为“非门”.

$\neg p$ 是数理逻辑中的标准记号，而在实际应用时常采用 $\bar{p}$ 记号，建议大家对这两种记号都要熟悉.

$\neg$ 是仅有的一个 1 元逻辑运算符，下面讨论的都是 2 元运算符.

3.2.2 合取联结词 $p\wedge q$

令 p：小李能歌，q：小李善舞，则 p 与 q 的**合取**(conjunction，and) $p\wedge q$：小李能歌并且善舞. 合取联结词 $\wedge$ 相当于自然语言中的“并且”、“与”、“和”、“以及”、“不但…而且…”、“虽然…但是…”、“尽管…仍然…”等. 合取联结词 $\wedge$ 的运算表如表 3-2 所示.

表 3-2

p	q	$p\wedge q$	p	q	$p\wedge q$
1	1	1	0	1	0
1	0	0	0	0	0

注意

(1) “小王和小李是同学”中的“和”没有合取之意.

(2) 在数理逻辑中，合取联结词 $\wedge$ 可以将任意两个命题联结起来以构造出新的命题，如用 p：$2+3=5$，q：今天上课，则 $p\wedge q$：$2+3=5$ 且今天上课. 下面要介绍的其他联结词都是这样理解.

$p\wedge q$ 可用 $p\&q$ 或 $p*q$ 表示，在 C 语言中用 $p\&\&q$ 表示，在数字逻辑以及计算机组成原理中 $p\wedge q$ 用 $p\cdot q$ 表示，并且约定“$\cdot$”可以省略，直接写成 pq，与其对应的门电路为“与门”.

3.2.3 析取联结词 $p\vee q$

令 p：这学期我选修人工智能课程，q：这学期我选修模式识别课程，则 p 与 q 的**析取**(disjunction，or) $p\vee q$：这学期我选修人工智能或模式识别课程. 析取联结词 $\vee$ 相当于自然语言中的“或”. 析取联结词 $\vee$ 的运算表如表 3-3 所示.

表 3-3

p	q	$p\vee q$	p	q	$p\vee q$
1	1	1	0	1	1
1	0	1	0	0	0

$p \vee q$ 在 C 语言中用 $p \| q$ 表示,在数字逻辑以及计算机组成原理中 $p \vee q$ 用 $p+q$ 表示,与其对应的门电路为“或门”.

否定、合取和析取是 3 种最基本的逻辑运算，是所有程序设计语言涉及的逻辑运算，在信息检索中会经常用到，可以按“(离散数学＋高等数学) * 视频”查询网页.

3.2.4 异或联结词 $p \oplus q$

自然语言中的“或”可能是“**可兼或**”(inclusive or),它表示两者可同时为真,用析取 ∨ 表示即可；也可能是“不可兼或”,它表示两者不能同时为真,换句话说,两者同时为真是假命题.这就需要异或联结词.

令 p:明天去深圳的飞机是上午 8:00 起飞,q:明天去深圳的飞机是上午 8:30 起飞,则 p 与 q 的**异或**(exclusive or, XOR) $p \oplus q$:明天去深圳的飞机是上午 8:00 或上午 8:30 起飞.异或联结词 ⊕ 的运算表如表 3-4 所示.

表 3-4

p	q	$p \oplus q$	p	q	$p \oplus q$
1	1	0	0	1	1
1	0	1	0	0	0

与异或联结词对应的门电路为“异或门”.

对于自然语言中的“或”用 ∨ 还是 ⊕ 需要仔细分析,一般来说,只要不是非常明显的不可兼就使用 ∨.

【例 3-2】 今天晚上我在寝室上自习或去电影院看电影.

解 令 p:今天晚上我在寝室上自习,q:今天晚上我去电影院看电影,则原命题可表示为 $p \vee q$.

【例 3-3】 本学期张三或李四当选为班长.

解 令 p:本学期张三当选为班长,q:本学期李四当选为班长,则原命题可表示为 $p \oplus q$.

3.2.5 条件联结词 $p \rightarrow q$

令 p:我有时间,q:我去看望我的父母,则 $p \rightarrow q$:如果我有时间,我就去看望我的父母.

$p \rightarrow q$ 读作“**p 蕴涵 q**”(implication)或“**p 条件 q**”(conditional),蕴涵联结词 → 相当于自然语言中的“若…则…”、“如果…那么…”等.蕴涵联结词 → 的运算表如表 3-5 所示.

表 3-5

p	q	$p \rightarrow q$	p	q	$p \rightarrow q$
1	1	1	0	1	1
1	0	0	0	0	1

$p \rightarrow q$ 在模糊逻辑系统中是标准的蕴涵联结词.蕴涵联结词也可以称为条件联结词,但是与 C 语言中的“条件运算”以及 if-then 语句含义不同.

在 $p \to q$ 中，p 称为**前件**（antecedent），q 称为**后件**（consequent）. 当前件为 1，后件为 1 时，$p \to q$ 为 1；当前件为 1，后件为 0 时，$p \to q$ 为 0，这两种情况下的取值是容易理解的. 又因为我们的→是实质蕴涵，规定在前件为 0，后件为 1 时，$p \to q$ 为 1；当前件为 0，后件为 0 时，$p \to q$ 为 1. 这样规定有其合理性，见下面的例子.

【例 3-4】 令 p：太阳从西边出来，q：$2+3=5$，则 $p \to q$："如果太阳从西边出来，那么 $2+3=5$"是真命题.

【例 3-5】 令 p：太阳从西边出来，q：$2+3=4$，则 $p \to q$："如果太阳从西边出来，那么 $2+3=4$"是真命题.

实际上，在根据子集的定义证明 1.1 节的定理 1-1：对于任意集合 A，有 $\varnothing \subseteq A$ 时，就要用到上述实质蕴涵的定义. 同样，在理解关系的自反、反自反、对称、反对称及传递性质时，也要用到上述实质蕴涵的定义.

当然，在现代逻辑中，对蕴涵的不同理解会得到不同的逻辑系统，如由严格蕴涵得出模态逻辑系统[10].

3.2.6 双条件联结词 $p \leftrightarrow q$

令 p：四边形是平行四边形，q：四边形的对边平行，则 $p \leftrightarrow q$：四边形是平行四边形当且仅当该四边形的对边平行. $p \leftrightarrow q$ 读作"**p 等价 q**"（equivalence）或"**p 双条件 q**"（biconditional），等价联结词↔相当于自然语言中的"当且仅当"、"充分必要条件"，其英文为 if and only if，缩写为 iff. 等价联结词↔的运算表如表 3-6 所示.

表 3-6

p	q	$p \leftrightarrow q$	p	q	$p \leftrightarrow q$
1	1	1	0	1	0
1	0	0	0	0	1

"p 当且仅当 q"有两层含义：(1)"p 当 q"是指 $q \to p$. (2)"p 仅当 q"是指 $p \to q$. 正因为此，等价联结词↔又可以称为双蕴涵联结词或双条件联结词.

在数字逻辑等课程中，等价联结词↔称为"同"，并用"⊙"符号表示，对应"同或门".

【例 3-6】 仅当你走，我留下.

解 令 p：我留下，q：你走，则原命题可表示为 $p \to q$.

在自然语言中，能用到的联结词就是上面 6 个. 但后面将证明，2 元逻辑运算还有下面 3 个，仅给出运算表.

3.2.7 与非联结词 $p \uparrow q$

$p \uparrow q$ 读作"**p 与非 q**"（NOT AND），它与下面的或非联结词"↓"（Peirce 箭头）相对应.

与非联结词以 Sheffer 的名字命名，称为 Sheffer 竖，而最初的记号为"|"，所以与非联结词"↑"的运算符号有些地方至今仍使用 Sheffer 竖符号"|". 在数字逻辑以及计算机组成原理中"↑"没有专用的运算符号，"p 与非 q"直接记为 $\overline{p \cdot q}$，对应的门电路为"与非门".

3.2.8 或非联结词 $p \downarrow q$

$p \downarrow q$ 读作"**p 或非 q**"(NOT OR),或非联结词"$\downarrow$"以 Peirce 的名字命名为"Peirce 箭头".

在数字逻辑以及计算机组成原理中"$\downarrow$"没有专用的运算符号,"p 或非 q"直接记为 $\overline{p+q}$,对应的门电路为"或非门".

3.2.9 条件否定联结词 $p \xrightarrow{n} q$

$p \xrightarrow{n} q$ 读作"**p 条件否定 q**"(NOT IF THEN),其中 n 表示否定 not.

"p 条件否定 q"可直接记为 $\neg(p \rightarrow q)$.

上面介绍了 1 个 1 元逻辑运算、8 个 2 元逻辑运算. 后面将证明：不同的 1 元逻辑运算和 2 元逻辑运算共 9 个.

要求 理解记忆上述 9 个,特别是最前面的 6 个联结词的运算表.

思考 如何定义 3 元逻辑运算?

习 题 3.2

1. (1) 设 p：现在很多人都有车,求 $\neg p$.

(2) 写出"-2 是偶数或 3 是正数"的否定命题.

(3) 设 p：每个自然数都是整数,求 $p \vee \neg p$.

2. 令 p：今天有雨,q：明天有雨,问 $p \wedge q$,$p \vee q$,$p \rightarrow q$,$p \oplus q$,$p \uparrow q$,$p \downarrow q$ 和 $p \xrightarrow{n} q$ 分别表示什么复合命题?

3. 令 p：我们去图书馆,q：我们去上网,问 $\neg(p \wedge q)$表示什么复合命题?

4. 令 p：我生病,q：我去上课,则"虽然我没有生病,但我不去上课"该如何用符号表示?

5. "张红和张兰是姐妹"中的和与联结词 $\wedge$ 有什么不同?

6. 写出一个命题,它可以表示为 $p \leftrightarrow (\neg q \wedge r)$.

3.3 命题公式及其真值表

有了前面的两节内容,就可以得到命题逻辑的符号体系. 由于所讲内容侧重于在后继课程中的应用,我们不给出逻辑演算系统的形式语言的定义.

3.3.1 命题公式的定义

命题公式就是逻辑函数或逻辑表达式,其中的常量是逻辑常量 1 和 0,其中的变元是命题变元或逻辑变量. 很快可以看到,这种逻辑函数的取值只可能为 1 或 0.

命题公式是由命题常量、命题变元、逻辑联结词、左圆括号"("及右圆括号")"构成的有意义(well-formed)的符号串,其严格定义常借助于递归定义方式给出.

【定义 3-1】 命题公式(proposition formula)集合按下列方法生成：

(1) 命题常量 1 和 0 以及命题变元是命题公式.

(2) 若 A 是命题公式,则$(\neg A)$是命题公式.

(3) 若 A 和 B 是命题公式,则$(A \wedge B)$,$(A \vee B)$,$(A \oplus B)$,$(A \rightarrow B)$,$(A \leftrightarrow B)$,$(A \uparrow B)$,$(A \downarrow B)$,$(A \xrightarrow{n} B)$是命题公式.

(4) 有限次应用(1)、(2)、(3)所得到的符号串是仅有的命题公式.

根据命题公式的定义知,p,$(\neg p)$,$(\neg(\neg p))$,$(1 \wedge p)$,$(0 \vee (\neg p))$,$(\neg(p \rightarrow q))$,$((p \oplus q) \downarrow q)$以及$(((p \vee q) \rightarrow r) \leftrightarrow ((\neg r) \rightarrow (p \wedge q)))$等是命题公式,而$(\neg(p \rightarrow))$,$(\neg p \rightarrow q))$等不是命题公式.

命题公式可称为**合式公式**(Well-Formed Formula, WFF)或简称为公式,其全称为命题合式公式.这儿的公式实际上是书写正确、含义清楚的表达式或者说符号串,与以前所学过的公式含义不尽一致.上面已经谈到,命题公式是逻辑函数(它与形式系统中的 WFF 的定义不尽一致),否则如 $A \wedge 1$ 及 $A \uparrow B$ 等就没有定义,可以借助于函数给命题公式下定义.

命题公式一般用 $A,B,C,\cdots$表示.若命题公式 A 中恰含有 n 个命题变元 $p_1,p_2,\cdots,p_n$,则可以将 A 记为 $A(p_1,p_2,\cdots,p_n)$.显然,命题公式 A 就是命题变元 $p_1,p_2,\cdots,p_n$ 的函数.

严格按照命题公式的定义,就会出现很多的括号.一方面,这些括号使命题公式的结构清晰、含义清楚;而另一方面,括号太多给命题公式的阅读和书写带来不便.因此,特作如下一些可以省略括号的约定:

(1) 最外层的括号可以省略.

在形成最终的命题公式时,所有的中间过程得到的命题公式,包含其本身,都称为该命题公式的**子公式**.如$((p \oplus q) \downarrow q)$的子公式分别为 p,q,$(p \oplus q)$和$((p \oplus q) \downarrow q)$.这条约定是说,在最终形成的命题公式$((p \oplus q) \downarrow q)$时,最外层的括号可以不写:$(p \oplus q) \downarrow q$,但在形成过程中的括号是至关重要的.

(2) 9 个联结词运算的优先顺序依次为

$$\neg, \wedge, \vee, \oplus, \rightarrow, \leftrightarrow, \uparrow, \downarrow, \xrightarrow{n}$$

符合本约定的有些括号可以不写.如命题公式

$$((p \vee q) \rightarrow r) \leftrightarrow ((\neg r) \rightarrow (p \wedge q))$$

可以写成

$$(p \vee q \rightarrow r) \leftrightarrow (\neg r \rightarrow p \wedge q)$$

或

$$p \vee q \rightarrow r \leftrightarrow \neg r \rightarrow p \wedge q$$

但这种优先顺序的规定不尽一致,如可以将 $\wedge$ 和 $\vee$ 看作同级别运算等[4].也可以按其他课本,只定义 5 个联结词$\neg$,$\wedge$,$\vee$,$\rightarrow$,$\leftrightarrow$从左至右的优先级别[8].

(3) 同级运算从左至右依次进行.如 $p \rightarrow q \rightarrow r$ 是$(p \rightarrow q) \rightarrow r$,但很多时候是写成$(p \rightarrow q) \rightarrow r$ 形式.

注意 “可以省略”表示也可以不省略,但在有些时候,把命题公式 $p \wedge q \rightarrow r$ 写成$(p \wedge q) \rightarrow r$ 也许更好.

实际上,在对命题进行符号化时,只要书写正确的逻辑函数都是命题公式.

3.3.2 命题的符号化

命题的符号化就是使用符号——命题变元、逻辑联结词和括号将所给出的命题表示出

来.一方面说明,符号体系来源于实际问题,另一方面也是给出进一步学习逻辑演算系统的语义解释时的一种标准模型.

命题的符号化的步骤:

(1) 找出所给命题的所有原子命题,并用小写英文字母或带下标表示.

(2) 确定应使用的联结词,进而将原命题用符号表示出来.

【例 3-7】 将下列命题符号化.

(1) 天气很好或很热.

(2) 如果张三和李四都不去,那么我就去.

(3) 仅当你走,我留下.

(4) 我今天进城,除非天下雨.

(5) 你只有刻苦学习,才能取得好成绩.

解 (1) 用 p: 天气很好, q: 天气很热, 则原命题符号化为: $p \vee q$.

本命题中的"或"不是明显的不可兼,所以用"$\vee$".

(2) 用 p: 张三去, q: 李四去, r: 我去, 则原命题符号化为: $\neg p \wedge \neg q \to r$.

注意 "张三不去"应是复合命题.

(3) 用 p: 你走, q: 我留下, 则原命题符号化为: $q \to p$.

(4) 用 p: 我今天进城, q: 天下雨, 则原命题符号化为: $\neg q \to p$.

"除非"相当于"如果不".

(5) 用 p: 你刻苦学习, q: 你取得好成绩, 则原命题符号化为: $q \to p$.

3.3.3 命题公式的真值表

对于命题公式 A,若对 A 中出现的每个命题变元都指定一个真值 1 或者 0,就对命题公式 A 进行了一种**真值指派**(assignment)或一个**解释**(interpretation),而在该指派下会求出公式 A 的一个真值.将 A 的所有可能的真值指派以及在每一个真值指派下的取值列成一个表,就得到命题公式 A 的**真值表**(truth table).

【例 3-8】 写出命题公式 $(\neg p \vee q) \to r$ 的真值表.

解 命题公式 $(\neg p \vee q) \to r$ 的真值指派共 8 种,分别为 $(p,q,r)=(1,1,1)$, $(1,1,0)$, $(1,0,1)$, $(1,0,0)$, $(0,1,1)$, $(0,1,0)$, $(0,0,1)$, $(0,0,0)$. 经过计算知,命题公式 $(\neg p \vee q) \to r$ 在指派下的取值分别为: 1, 0, 1, 1, 1, 0, 1, 0. 因此,命题公式 $(\neg p \vee q) \to r$ 的真值表如表 3-7 所示.

表 3-7

p	q	r	$\neg p$	$\neg p \vee q$	$(\neg p \vee q) \to r$	p	q	r	$\neg p$	$\neg p \vee q$	$(\neg p \vee q) \to r$
1	1	1	0	1	1	0	1	1	1	1	1
1	1	0	0	1	0	0	1	0	1	1	0
1	0	1	0	0	1	0	0	1	1	1	1
1	0	0	0	0	1	0	0	0	1	1	0

在列真值表时,最好将中间的计算过程也写出来,如表 3-7 中的第 4 列和第 5 列,它实

际上是按命题公式的形成过程(或者说是按命题公式的层)书写的,关键是列举所有真值指派及在每一种指派下的取值.

正因为这样,在列真值表时主要是所有命题变元及其真值指派和在每种指派下命题公式的取值.在当一个命题公式较复杂时,有些子公式可以省略.也可以将所有命题变元及其真值指派都放在第一列.这实际上是一种简化的真值表.

要求大家能准确写出一个命题公式的真值表,这是本节的重点内容,当然必须牢记联结词的运算表才行.

由表 3-7 知,含 3 个命题变元的命题公式有 $8=2^3$ 种不同的真值指派.很显然,含 2 个命题变元的命题公式有 $4=2^2$ 种不同的真值指派.一般来说,含 $n(n\geqslant 1)$个命题变元的命题公式的不同的真值指派有 2^n 种.

思考 设计程序,对于给定的命题公式构造真值表.

3.3.4 命题公式的类型

【定义 3-2】 在任何指派下均取真的命题公式称为**永真式**或**重言式**(tautology);在任何指派下均取假的命题公式称为**永假式**或**矛盾式**(contradiction);至少有一种指派使其为真的命题公式称为**可满足式**(satisfactable formula);至少有一种指派使其为真同时至少有一种指派使其为假的命题公式称为**中性式**或**偶然式**(contingency).

根据定义知,命题公式$(\neg p\vee q)\rightarrow r$ 为中性式.很容易验证,命题公式 $p\vee\neg p$ 为永真式,$p\wedge\neg p$ 为永假式.

命题公式的分类如下:

$$命题公式\begin{cases}可满足式\begin{cases}永真式\\中性式\end{cases}\\永假式\end{cases}$$

显然,A 永真的充要条件是$\neg A$ 永假;$A\wedge B$ 永真的充要条件是 A 和 B 均永真.

永真式是非常重要的一类命题公式,先看一个例子.

【例 3-9】 证明:命题公式$(p\rightarrow q)\leftrightarrow(\neg p\vee q)$是永真式.

证 列出$(p\rightarrow q)\leftrightarrow(\neg p\vee q)$的真值表如表 3-8 所示.

表 3-8

p	q	$p\rightarrow q$	$\neg p$	$\neg p\vee q$	$(p\rightarrow q)\leftrightarrow(\neg p\vee q)$
1	1	1	0	1	1
1	0	0	0	0	1
0	1	1	1	1	1
0	0	1	1	1	1

由真值表可知,命题公式$(p\rightarrow q)\leftrightarrow(\neg p\vee q)$是永真式.

注意 利用真值表得出一个命题公式的类型是最常用的方法,这种方法可以称为**真值表法**.

真值表法,从理论上来说,是完全可行的,但当命题变元较多时也是极为不方便的,例如

当你编一个程序来做这件事时就会遇到这样的需要解决的问题.

【例 3-10】 证明:命题公式$(p\wedge(p\rightarrow q))\rightarrow q$是永真式.

证 假设$p\wedge(p\rightarrow q)$取真,则p及$p\rightarrow q$均取真,进而q为真,因此$(p\wedge(p\rightarrow q))\rightarrow q$永真.

同例 3-9 一样,可以利用真值表法对例 3-10 进行证明,但对于证明$A\rightarrow B$永真,可以通过"取值"的方法证明:"由A真推出B真或由B假推出A假,则$A\rightarrow B$永真",因为这意味着不可能出现"A真B假"情形.

注意 这种利用取值的方法得出一个命题公式的类型可以称为**取值法**.

取值法本质上是真值表方法,但它与真值表法是有一些区别的.若能用好这种方法,对于证明有些结论是非常方便的,参见本节的习题第 3、4、6 题.

最后介绍永真式的代入定理(Rule of Substitution,RS).

【定理 3-1】(永真式代入定理) 设命题公式$A(p_1,p_2,\cdots,p_n)$为永真式,则分别用命题公式$B_1,B_2,\cdots,B_n$全部代换A中的命题变元$p_1,p_2,\cdots,p_n$所得到的命题公式(称为A的代入实例,substitution instance)是永真式.

证 设替换后的命题公式为B,对于公式B的任意一种指派,命题公式$B_1,B_2,\cdots,B_n$有真值$t_1,t_2,\cdots,t_n$,而由已知,显然有$A(t_1,t_2,\cdots,t_n)$取真,所以B是永真式.证毕.

永真式的代入定理是这样使用的:由于命题公式$(p\rightarrow q)\leftrightarrow(\neg p\vee q)$是永真式,对于任意命题公式$A$和$B$,根据代入定理知,$(A\rightarrow B)\leftrightarrow(\neg A\vee B)$是永真式;由于命题公式$(p\wedge(p\rightarrow q))\rightarrow q$是永真式,所以$(A\wedge(A\rightarrow B))\rightarrow B$是永真式.

从代入定理的证明知,要证明对于任意命题公式A和B,$(A\rightarrow B)\leftrightarrow(\neg A\vee B)$是永真式,原则上可以将$A$和$B$看作命题变元,不过在用真值表法证明永真时最好先就命题变元进行,再利用永真式的代入定理(请思考为什么).

习 题 3.3

1. 将下列命题符号化.

(1) 若a和b是奇数,则$a+b$是偶数.

(2) 只有在正整数$n\leqslant 2$时,不定方程$x^n+y^n=z^n$才有正整数解.

(3) 天在下雨,我没有去书店.

(4) 两矩阵相等当且仅当其对应的元素分别相等.

(5) 这苹果虽然甜,但我不打算买.

(6) 除非我接到正式邀请,否则我不去参加圣诞晚会.

(7) 我和小王是同学.

(8) 因为他要看今晚的 NBA 篮球比赛,所以他没有来上自习.

(9) 尽管她学习成绩不太好,但她的动手能力很强.

(10) 我的手机没电了,借你的手机用一下.

2. 设p,q和r为命题变元,列出下列命题公式的真值表.

(1) $(\neg p\wedge(p\vee q))\rightarrow q$.

(2) $(\neg p\vee\neg q)\rightarrow(p\leftrightarrow\neg q)$.

(3) $(p\vee q)\rightarrow r$.

(4) $(p\to(q\wedge r))\wedge(\neg p\to(\neg q\wedge\neg r))$.

3. 设 p,q,r 和 s 为命题变元,判断下列命题公式的类型.

(1) $(p\to(q\to r))\leftrightarrow((p\wedge q)\to r)$.

(2) $((p\to r)\vee\neg r)\to(\neg(q\to p)\wedge q)$.

(3) $((p\vee q)\to r)\leftrightarrow(r\to(p\wedge q))$.

(4) $p\to(\neg p\wedge q\wedge r\wedge s)$.

4. 证明:对于任意命题公式 A,B 和 C,下列命题公式均永真.

(1) $A\to(B\to A)$.

(2) $(A\to(B\to C))\to((A\to B)\to(A\to C))$.

(3) $(\neg A\to\neg B)\to(B\to A)$.

5. 证明:对于任意命题公式 A 和 B,有$(A\leftrightarrow B)\leftrightarrow(A\to B)\wedge(B\to A)$永真.

6. 对于任意命题公式 A、B 和 C,证明下列命题公式永真.

(1) $\neg A\to(A\to B)$.

(2) $(A\vee B)\wedge(A\to C)\wedge(B\to C)\to C$.

(3) $(A\to B)\wedge(A\to\neg B)\to\neg A$.

(4) $A\to(\neg A\to B)$.

3.4 逻辑等值的命题公式

将一个命题,如“四边形的对边平行”转换成与之逻辑等价的命题“四边形的对边相等”,所谓逻辑等价是指由“四边形的对边平行”可得出“四边形的对边相等”,且由“四边形的对边相等”可得出“四边形的对边平行”. 显然,这两个命题的真值是相同的,这时称这两个命题是逻辑等值的.

下面讨论两个命题公式逻辑等值.

3.4.1 逻辑等值的定义

【定义 3-3】 给定两个命题公式 A 和 B,若在任何真值指派下 A 和 B 的真值都相同,则称命题公式 A 和 B **逻辑等值**(logically equal)或逻辑等价(logically equivalent),简称为等值或相等,记为 $A=B$.

首先注意到,结合上面的例子容易知道 $A=B$ 意味着 A 和 B 是逻辑等价(logically equivalent)的,它表示的是两个公式之间的一种关系,也可记为 $A\Leftrightarrow B$,它们仅是考虑问题的角度不同而已.

尽管在逻辑演算系统中,等号“=”有其特殊的用途,但在后继课程中通常都是从取逻辑值的角度讨论两个逻辑函数或逻辑表达式 A 和 B 是否相等,用 $A=B$ 的时候更多. 本书大多数时候用 $A=B$,有时候也用 $A\Leftrightarrow B$.

习惯上所说的(两个命题)等价实际上是指它们逻辑等价,请不要与等价联结词“$\leftrightarrow$”混淆了,后者仅是一个运算符号,运算的结果可真可假,而两个命题公式等价是指逻辑等价. 因为有下面的定理 3-2,所以逻辑等价又称为重言等价,重言等价中的联结词是“$\leftrightarrow$”.

注意 “=”或“$\Leftrightarrow$”是关系符号,$A=B$ 是等值式;“$\leftrightarrow$”是运算符号,$A\leftrightarrow B$ 是命题公式.

【定理 3-2】 设 A 和 B 是命题公式，则 $A=B$ 的充要条件是 $A\leftrightarrow B$ 为永真式.

证 （$\Rightarrow$）由 $A=B$ 可知，A 和 B 的真值是相同的，所以 $A\leftrightarrow B$ 为永真式.

（$\Leftarrow$）若 $A\leftrightarrow B$ 为永真式，则 A 和 B 的真值相同，因此 $A=B$.

下面的例子说明如何利用真值表证明两个命题公式等值.

【例 3-11】 证明：对于任意命题公式 A 和 B，有 $A\rightarrow B=\neg A\vee B$.

证 先证明，对于命题变元 p 和 q，有 $p\rightarrow q=\neg p\vee q$.

为便于比较，将命题公式 $p\rightarrow q$ 和 $\neg p\vee q$ 的真值表列在同一张表中，如表 3-9 所示.

表 3-9

p	q	$p\rightarrow q$	$\neg p$	$\neg p\vee q$
1	1	1	0	1
1	0	0	0	0
0	1	1	1	1
0	0	1	1	1

由表 3-9 知，命题公式 $p\rightarrow q$ 和 $\neg p\vee q$ 的真值在任何情况下都是相同的，根据命题公式等值的定义有 $p\rightarrow q=\neg p\vee q$.

由于 $p\rightarrow q=\neg p\vee q$，根据定理 3-2 知 $(p\rightarrow q)\leftrightarrow(\neg p\vee q)$ 永真，由永真式代入定理（定理 3-1）知，对于任意的命题公式 A 和 B，$(A\rightarrow B)\leftrightarrow(\neg A\vee B)$ 永真（参照例 3-9），于是 $A\rightarrow B=\neg A\vee B$.

从例子的最后说明可知有下述定理：

【定理 3-3】 若 $A_1(p_1,p_2,\cdots,p_n)=A_2(p_1,p_2,\cdots,p_n)$，在 A_1 和 A_2 中分别用命题公式 $B_1,B_2,\cdots,B_n$ 去代换 $p_1,p_2,\cdots,p_n$ 所得到的两个命题公式等值.

命题公式之间的等值是命题公式间的一种关系，很显然有下面的定理.

【定理 3-4】 命题公式间的等值关系是等价关系：对任意命题公式 A,B,C 有：

（1）$A=A$（自反性）；

（2）若 $A=B$，则 $B=A$（对称性）；

（3）若 $A=B$ 且 $B=C$，则 $A=C$（传递性）.

3.4.2 基本等值式

1. 与 $\neg,\wedge,\vee$ 有关的等值式

【定理 3-5】 设 A,B,C 是任意的命题公式，则命题的 $\vee,\wedge,\neg$ 运算有下列重要性质：

（1）$\neg\neg A=A$（**对合律**）.

（2）$A\vee A=A,A\wedge A=A$（**幂等律**或称为**重叠律**）.

（3）$A\vee B=B\vee A$，$A\wedge B=B\wedge A$（**交换律**）.

（4）$(A\vee B)\vee C=A\vee(B\vee C)$，$(A\wedge B)\wedge C=A\wedge(B\wedge C)$（**结合律**）.

（5）$A\vee(A\wedge B)=A,A\wedge(A\vee B)=A$（**吸收律**）.

（6）$A\vee(B\wedge C)=(A\vee B)\wedge(A\vee C),A\wedge(B\vee C)=(A\wedge B)\vee(A\wedge C)$（**分配律**）.

（7）$A\vee\neg A=1,A\wedge\neg A=0$（**互补律**：$A$ 有补元 $\overline{A}$）.

(8) $\neg(A\vee B)=\neg A\wedge\neg B$, $\neg(A\wedge B)=\neg A\vee\neg B$ (**De Morgan 律**).

(9) $A\vee 0=0\vee A=A$, $A\wedge 1=1\wedge A=A$($\vee$, $\wedge$有**单位元**或称为同一律).

(10) $A\vee 1=1\vee A=1$, $A\wedge 0=0\wedge A=0$($\vee$, $\wedge$有**零元**或称为 0-1 律).

上面关于命题的$\vee$, $\wedge$, $\neg$运算性质与集合的$\cup$, $\cap$, $\bar{\ }$运算性质是完全类似的,这也是将命题逻辑等有关内容安排在第 1、2 章之后的原因之一. 实际上,这种现象不是偶然的,它们之间有密切的联系,参见第 5 章.

上面的每一条性质都可以借助于真值表技术加以证明. 下面仅举一例加以说明.

【例 3-12】 证明:对于任意命题公式 A 和 B,有 $A\vee(A\wedge B)=A$ 成立.

证 根据定理 3-3,只需证明,对于命题变元 p 和 q,吸收律 $p\vee(p\wedge q)=p$ 成立即可. 列出命题公式 $p\vee(p\wedge q)$和 p 的真值表,如表 3-10 所示.

表 3-10

p	q	$p\wedge q$	$p\vee(p\wedge q)$	p	q	$p\wedge q$	$p\vee(p\wedge q)$
1	1	1	1	0	1	0	0
1	0	0	1	0	0	0	0

由表 3-10 知,$p\vee(p\wedge q)$和 p 的真值在任何真值指派下都相同,所以 $p\vee(p\wedge q)=p$.

2. 其他重要的等值式

【定理 3-6】 设 A,B 是任意的命题公式,则

(1) $A\oplus B=\neg(A\leftrightarrow B)=(A\wedge\neg B)\vee(\neg A\wedge B)$.

(2) $A\rightarrow B=\neg A\vee B$.

(3) $A\leftrightarrow B=(A\rightarrow B)\wedge(B\rightarrow A)$.

(4) $A\uparrow B=\neg(A\wedge B)$.

(5) $A\downarrow B=\neg(A\vee B)$.

(6) $A\overset{n}{\rightarrow}B=\neg(A\rightarrow B)$.

证 只证(3),其余留作练习. 需要证明:对于命题变元 p 和 q,有 $p\leftrightarrow q=(p\rightarrow q)\wedge(q\rightarrow p)$. 列出 $p\leftrightarrow q$ 和$(p\rightarrow q)\wedge(q\rightarrow p)$的真值表,如表 3-11 所示.

表 3-11

p	q	$p\leftrightarrow q$	$p\rightarrow q$	$q\rightarrow p$	$(p\rightarrow q)\wedge(q\rightarrow p)$
1	1	1	1	1	1
1	0	0	0	1	0
0	1	0	1	0	0
0	0	1	1	1	1

由表 3-11 可知,命题公式 $p\leftrightarrow q$ 和$(p\rightarrow q)\wedge(q\rightarrow p)$在任意指派下的取值都相同,从而由等值的定义知 $p\leftrightarrow q=(p\rightarrow q)\wedge(q\rightarrow p)$,进而 $A\leftrightarrow B=(A\rightarrow B)\wedge(B\rightarrow A)$.

关于逻辑联结词$\oplus$,$\rightarrow$,$\leftrightarrow$,$\uparrow$,$\downarrow$,$\overset{n}{\rightarrow}$,还有很多其他性质,例如$\oplus$,$\leftrightarrow$,$\uparrow$,$\downarrow$满足交换律等,请大家根据运算具有的性质(1.3 节)自己进行总结,这是一件很值得去做的事情,部分性质见习题.

3.4.3 等值演算法

基本等值式有很多用途，如化简命题公式、判断命题公式的类型、证明等值式、计算命题公式的范式、命题逻辑中的推理等，要求大家要熟记，特别是定理 3-6 中的等值式.

在使用等值式时，下列的等值置换定理(Rule of Replacement，RR)是至关重要的，它的证明是显然的.

【定理 3-7】(等值置换定理) 设 C 是命题公式 A 的子公式且 $C=D$，则将 A 中的 C 部分或全部替换成 D 所得到的命题公式与 A 等值.

利用基本等值式以及等值置换定理求解问题的方法称为**等值演算法**.

【例 3-13】 设 A,B,C 是任意的命题公式，化简下列命题公式并将最后结果用只含 $\neg$ 和 $\vee$ 表示.

(1) $(A\to(B\vee\neg C))\wedge\neg A\wedge B$.

(2) $\neg A\wedge\neg B\wedge(\neg C\to A)$.

解 (1) $(A\to(B\vee\neg C))\wedge\neg A\wedge B=(\neg A\vee(B\vee\neg C))\wedge\neg A\wedge B$

$$=((\neg A\vee(B\vee\neg C))\wedge\neg A)\wedge B\overset{\text{吸收律}}{=\!=\!=}\neg A\wedge B=\neg(A\vee\neg B).$$

(2) $\neg A\wedge\neg B\wedge(\neg C\to A)=\neg A\wedge\neg B\wedge(\neg\neg C\vee A)$

$$=(\neg A\wedge\neg B)\wedge(C\vee A)\overset{\text{分配律}}{=\!=\!=}(\neg A\wedge\neg B\wedge C)\vee(\neg A\wedge\neg B\wedge A)$$

$$=(\neg A\wedge\neg B\wedge C)\vee 0=\neg A\wedge\neg B\wedge C=\neg(A\vee B\vee\neg C).$$

说明 命题公式的化简是指将其化为一个与其等值的满足条件的含"联结词最少"的命题公式.

利用等值演算法，判断一个命题公式的类型是比较方便的.

【例 3-14】 设 A,B,C 是任意的命题公式，判断下列命题公式的类型.

(1) $(A\to(B\to C))\leftrightarrow((A\wedge B)\to C)$.

(2) $A\to(\neg A\wedge B\wedge C)$.

解 (1) 因为 $A\to(B\to C)=A\to(\neg B\vee C)=\neg A\vee(\neg B\vee C)=(\neg A\vee\neg B)\vee C=\neg(A\wedge B)\vee C=(A\wedge B)\to C$，所以$(A\to(B\to C))\leftrightarrow((A\wedge B)\to C)$是永真式.

(2) 因为 $A\to(\neg A\wedge B\wedge C)=\neg A\vee(\neg A\wedge B\wedge C)=\neg A\vee(\neg A\wedge(B\wedge C))=\neg A$，而 $\neg A$ 是中性式，因此 $A\to(\neg A\wedge B\wedge C)$是中性式.

两个命题公式等值，可以根据定义，利用真值表进行证明. 下面是证明两个命题公式等值的等值演算法.

【例 3-15】 设 A,B,C 是任意的命题公式，证明下列等值式.

(1) $\neg(A\leftrightarrow B)=(A\vee B)\wedge(\neg A\vee\neg B)$.

(2) $A\to(B\vee C)=(A\wedge\neg B)\to C$.

证 (1) $\neg(A\leftrightarrow B)=\neg((A\to B)\wedge(B\to A))=\neg((\neg A\vee B)\wedge(\neg B\vee A))$

$$=\neg(\neg A\vee B)\vee\neg(\neg B\vee A)=(A\wedge\neg B)\vee(B\wedge\neg A)$$

$$=((A\wedge\neg B)\vee B)\wedge((A\wedge\neg B)\vee\neg A)$$

$$=(A\vee B)\wedge(\neg B\vee B)\wedge(A\vee\neg A)\wedge(\neg B\vee\neg A)$$

$$=(A\vee B)\wedge(\neg A\vee\neg B).$$

(2) $A\rightarrow(B\vee C)=\neg A\vee(B\vee C)=(\neg A\vee B)\vee C$

$$=\neg(A\wedge\neg B)\vee C=(A\wedge\neg B)\rightarrow C.$$

3.4.4 对偶原理

在定理 3-5 中,除性质(1)外,其他性质都是成对出现的,两者间有一定的联系.先给出命题公式的对偶式的定义.

【定义 3-4】 设命题公式 A 中至多含 3 个逻辑联结词 $\neg$, $\wedge$, $\vee$,将 A 中的 $\wedge$ 换成 $\vee$;A 中的 $\vee$ 换成 $\wedge$;A 中的 1 换成 0;A 中的 0 换成 1,所得到的命题公式称为是 A 的**对偶式**(dual formula),记为 A^*.

【例 3-16】 设 p,q 和 r 是命题变元,分别求下列命题公式的对偶式.

(1) $\neg(p\wedge q)\wedge 1$.

(2) $p\vee(q\wedge r)$.

解 (1) $\neg(p\wedge q)\wedge 1$ 的对偶式为 $\neg(p\vee q)\vee 0$.

(2) $p\vee(q\wedge r)$的对偶式为 $p\wedge(q\vee r)$.

注意 一般来说,$A\neq A^*$.

根据 De Morgan 律可以证明下面的对偶定理.

【定理 3-8】(对偶原理) 设 A 和 B 是命题公式,若 $A=B$,则 $A^*=B^*$.

有了对偶原理后,定理 3-5 中除性质(1)外的等值式,只需要记住其中一个就可以了.例如,因为 $\neg(p\vee q)=\neg p\wedge\neg q$,由对偶原理可得 $\neg(p\wedge q)=\neg p\vee\neg q$.

同时,有了对偶原理,我们可以求出任意命题公式的对偶式.例如,因为 $p\rightarrow q=\neg p\vee q$,所以 $p\rightarrow q$ 的对偶式等于 $\neg p\vee q$ 的对偶式,于是 $p\rightarrow q$ 的对偶式为 $\neg p\wedge q$.

习 题 3.4

1. 证明:命题公式间的等值关系是等价关系.
2. 证明定理 3-5 中的分配律(6)和 De Morgan 律(8).
3. 设 A,B,C 是任意的命题公式,判断下列命题是否成立,阐述理由.

(1) 若 $A\wedge C=B\wedge C$,则 $A=B$.

(2) 若 $A\vee C=B\vee C$,则 $A=B$.

(3) 若 $\neg A=\neg B$,则 $A=B$.

4. 设 A,B 是任意的命题公式,证明下列各式.

(1) $A\oplus B=\neg(A\leftrightarrow B)=(A\wedge\neg B)\vee(\neg A\wedge B)$.

(2) $A\rightarrow B=\neg A\vee B$.

(3) $A\uparrow B=\neg(A\wedge B)$.

(4) $A\downarrow B=\neg(A\vee B)$.

5. 设 A,B,C 是任意的命题公式,证明下列各式.

(1) $A\oplus B=B\oplus A$.

(2) $(A\oplus B)\oplus C=A\oplus(B\oplus C)$.

(3) $A\rightarrow B=\neg B\rightarrow\neg A$.

(4) $\neg(A\leftrightarrow B)=A\leftrightarrow\neg B$.

6. 设 A 和 B 是命题公式,关于逻辑联结词 $\uparrow$ 有下述结论,证明下列各式.

(1) $\neg A=A\uparrow A$.

(2) $A\wedge B=(A\uparrow B)\uparrow(A\uparrow B)$.

(3) $A\vee B=(A\uparrow A)\uparrow(B\uparrow B)$.

7. 设 A 和 B 是命题公式,关于逻辑联结词 $\downarrow$ 有下述结论,证明下列各式.

(1) $\neg A=A\downarrow A$.

(2) $A\wedge B=(A\downarrow A)\downarrow(B\downarrow B)$.

(3) $A\vee B=(A\downarrow B)\downarrow(A\downarrow B)$.

8. 设 A, B 和 C 是命题公式,将等价联结词$\leftrightarrow$记为$\odot$,证明下列各式.

(1) $A\odot B=B\odot A$.

(2) $(A\odot B)\odot C=A\odot(B\odot C)$.

(3) $A\odot B=\neg(A\oplus B)$.

(4) $A\odot B=(A\wedge B)\vee(\neg A\wedge\neg B)$.

9. 设 A,B,C,D 是任意的命题公式,化简下列命题公式并将最后结果仅用 $\downarrow$ 表示.

(1) $(A\wedge B\wedge C)\vee(A\wedge\neg B\wedge C)$.

(2) $(A\wedge B)\vee(\neg A\wedge B)\vee(A\wedge\neg B)$.

(3) $\neg((A\wedge B)\vee(A\wedge C))$.

(4) $(A\wedge B)\vee(\neg A\wedge B)\vee(B\wedge C\wedge D)$.

10. 设 A,B,C,D 是任意的命题公式,判断下列命题公式的类型.

(1) $((A\rightarrow C)\vee\neg C)\rightarrow(\neg(B\rightarrow A)\wedge A)$.

(2) $(A\rightarrow C)\rightarrow((B\rightarrow D)\rightarrow((A\vee B)\rightarrow C))$.

11. 设 A,B,C 是任意的命题公式,证明下列等值式.

(1) $\neg(A\rightarrow B)=A\wedge\neg B$.

(2) $A\rightarrow(B\rightarrow A)=\neg A\rightarrow(A\rightarrow\neg B)$.

(3) $(A\rightarrow C)\wedge(B\rightarrow C)=(A\vee B)\rightarrow C$.

(4) $A\rightarrow(B\rightarrow C)=(A\wedge B)\rightarrow C$.

12. 设 p 和 q 是命题变元,试求出 $p\oplus q$ 的对偶式,它与 $p\odot q$ 的关系如何?

13. 有一个国家只有两种人:一种人总说真话,一种人总说假话.一个逻辑学家来到该国,在一个三岔路口处,不知道哪一条路是去首都方向的.这时碰巧来了一个人,逻辑学家只问了他一个问题,就知道去首都的路了.请问他问的是什么问题?为什么?

3.5 命题公式的范式

给定一个命题公式,根据其真值表显然可以方便地得出其在每种指派下的真值,从理论上讲,这是一个能行可判定问题.但随着所给公式中命题变元个数的增加,在实际计算中就变成不可行的了,例如含 100 个命题变元的命题公式其真值指派就有 2^{100} 种.

由第 3.4 节知,等值关系是等价关系,需要考虑其等价类及其代表元.一个命题公式有各种形式的与其等值的命题公式,在它们中间欲找到一种标准形式或规范形式,也就是命题

公式的范式,使其不用写出真值表就能确定在何真值指派下取真以及在何真值指派下取假.

3.5.1 命题公式的析取范式及合取范式

1. 析取范式及合取范式的定义

【定义 3-5】 设 A 是命题公式,若 $A=A_1 \vee A_2 \vee \cdots \vee A_n(n \geqslant 1)$,其中 $A_i(1 \leqslant i \leqslant n)$是由命题变元或其否定组成的合取式,则称 $A_1 \vee A_2 \vee \cdots \vee A_n$ 为命题公式 A 的**析取范式**(disjunctive normal form).

关于析取范式的定义,需注意如下两点.

注意

(1) $A_i(1 \leqslant i \leqslant n)$是由命题变元或其否定组成的合取式.例如,$A_i(1 \leqslant i \leqslant n)$可以是 $\neg p \wedge \neg q \wedge r, p \wedge \neg q, \neg q \wedge r$ 等,也可以是单个的命题变元或其否定,如 $q, \neg r$ 等.但最好满足:

① 在每个 A_i 中,命题变元及其否定不同时出现,否则 $A_i=0$,在 A 的析取范式中可以消去该合取式;

② 在每个 A_i 中,命题变元或其否定按字典顺序出现或按下标从小到大顺序出现;

③ 相同的析取式不重复出现,因为 $\vee$ 运算具有幂等性,如$(p \wedge \neg q) \vee (p \wedge \neg q)=(p \wedge \neg q)$.

(2) A 的析取范式 $A_1 \vee A_2 \vee \cdots \vee A_n$ 中,n 可以为 1.也就是说,单个由命题变元或其否定组成的析取式看成一个整体是命题公式 A 的析取范式,例如若 $A=\neg p \wedge \neg q \wedge r$,则$(\neg p \wedge \neg q \wedge r)$是 A 的析取范式.

类似地可以给出命题公式的合取范式的定义.

【定义 3-6】 设 A 是命题公式,若 $A=A_1 \wedge A_2 \wedge \cdots \wedge A_n(n \geqslant 1)$,其中 $A_i(1 \leqslant i \leqslant n)$是由命题变元或其否定组成的析取式,则称 $A_1 \wedge A_2 \wedge \cdots \wedge A_n$ 为命题公式 A 的**合取范式**(conjunctive normal form).

同样,关于合取范式的定义,也需注意两点.

注意

(1) $A_i(1 \leqslant i \leqslant n)$是由命题变元或其否定组成的析取式.例如,$A_i(1 \leqslant i \leqslant n)$可以是 $\neg p \vee \neg q \vee r, p \vee \neg q, \neg q \vee r$ 等,也可以是单个的命题变元或其否定,如 $q, \neg r$ 等.但最好满足:

① 在每个 A_i 中,命题变元及其否定不同时出现,否则 $A_i=1$,在 A 的合取范式中可以消去该析取式;

② 在每个 A_i 中,命题变元或其否定按字典顺序出现或按下标从小到大顺序出现;

③ 相同的析取式不重复出现,因为 $\wedge$ 运算具有幂等性,如$(p \vee \neg q) \wedge (p \vee \neg q)=(p \vee \neg q)$.

(2) A 的合取范式 $A_1 \wedge A_2 \wedge \cdots \wedge A_n$ 中,n 可以为 1.也就是说,单个由命题变元或其否定组成的析取式看成一个整体是命题公式 A 的合取范式,例如若 $A=\neg p \vee \neg q \vee r$,则$(\neg p \vee \neg q \vee r)$是 A 的合取范式.

由定义可知,若 $A=\neg p \vee \neg q \vee r$,则 $\neg p \vee \neg q \vee r=(\neg p \vee \neg q \vee r)$是 A 的合取范式,$\neg p \vee \neg q \vee r=(\neg p) \vee (\neg q) \vee (r)$也是 A 的析取范式.

2. 析取范式及合取范式的计算

计算命题公式的析取范式及合取范式的主要步骤如下.

(1) 使用等值式,将命题公式中的联结词归约为$\neg$,$\wedge$,$\vee$.

(2) 利用 De Morgan 律将$\neg$移到命题变元的前面.

(3) 根据分配律得到命题公式的析取范式及合取范式.

$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)\text{(求析取范式用)}$$

$$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)\text{(求合取范式用)}$$

【例 3-17】 设 p,q 和 r 是命题变元,求命题公式 $A=(p\rightarrow q)\leftrightarrow r$ 的析取范式及合取范式.

解 求命题公式的析取范式及合取范式的步骤 1 和步骤 2 是相同的.

$$\begin{aligned}A &= (p\rightarrow q)\leftrightarrow r = (\neg p \vee q)\leftrightarrow r\\ &= ((\neg p \vee q)\rightarrow r)\wedge(r\rightarrow(\neg p\vee q))\\ &= (\neg(\neg p \vee q) \vee r) \wedge (\neg r \vee (\neg p \vee q)) \quad \text{(步骤 1 结束)}\\ &= ((p \wedge \neg q) \vee r) \wedge (\neg p \vee q \vee \neg r) \quad \text{(步骤 2 完成)}\end{aligned}$$

(1) 析取范式.

$$\begin{aligned}A &= (\underline{(p \wedge \neg q)} \vee \underline{r}) \wedge \underline{(\neg p \vee q \vee \neg r)}\\ &= (\underline{(p \wedge \neg q)} \wedge (\underline{\neg p} \vee \underline{q} \vee \underline{\neg r})) \vee (\underline{r} \wedge (\underline{\neg p} \vee \underline{q} \vee \underline{\neg r}))\\ &= ((p \wedge \neg q) \wedge \neg p) \vee ((p \wedge \neg q) \wedge q) \vee ((p \wedge \neg q) \wedge \neg r)\\ &\quad \vee (r \wedge \neg p) \vee (r \wedge q) \vee (r \wedge \neg r)\\ &= (p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge r) \vee (q \wedge r)\end{aligned}$$

(2) 合取范式.

$$\begin{aligned}A &= ((\underline{p} \wedge \underline{\neg q}) \vee \underline{r}) \wedge (\neg p \vee q \vee \neg r)\\ &= (p \vee r) \wedge (\neg q \vee r) \wedge (\neg p \vee q \vee \neg r)\end{aligned}$$

从计算命题公式的析取范式及合取范式的步骤知道,任意命题公式都存在析取范式及合取范式.

3. 析取范式及合取范式的应用

根据命题公式的析取范式及合取范式可分别得出该命题公式取真、假的指派,例如在例 3-17 中,已求得 A 的析取范式为$A=(p\wedge\neg q\wedge\neg r)\vee(\neg p\wedge r)\vee(q\wedge r)$,若 A 取 1,则$(p\wedge\neg q\wedge\neg r)$,$(\neg p\wedge r)$,$(q\wedge r)$至少一个为 1,而它们都是合取式,由$p\wedge\neg q\wedge\neg r=1$,则$(p,q,r)=(1,0,0)$,由$\neg p\wedge r=1$,则 $p=0,r=1$,进而$(p,q,r)=(0,1,1),(0,0,1)$,由 $q\wedge r=1$,则 $q=1,r=1$,进而$(p,q,r)=(1,1,1),(0,1,1)$,于是,使 A 取 1 的指派有

$$(p,q,r) = (1,0,0),(0,1,1),(0,0,1),(1,1,1)$$

同样,由 A 的合取范式为$A=(p\vee r)\wedge(\neg q\vee r)\wedge(\neg p\vee q\vee\neg r)$可得出使 A 取 0 的指派有

$$(p,q,r) = (1,0,1),(1,1,0),(0,1,0),(0,0,0)$$

【例 3-18】 从 p,q,r,s 4 个人中选派 2 人出差,求满足下列 3 个条件的选派方法有哪几种.

(1) 若 p 去,则 r 和 s 中只去 1 人;

(2) q 和 r 不能都去；

(3) 若 r 去则 s 不能去.

解 p：p 去出差，q：q 去出差，r：r 去出差，s：s 去出差，则 $p\rightarrow(r\oplus s)$，$\neg(q\wedge r)$，$r\rightarrow\neg s$同时成立.

令

$$A=(p\rightarrow(r\oplus s))\wedge\neg(q\wedge r)\wedge(r\rightarrow\neg s)$$

因为 $r\oplus s=(r\wedge\neg s)\vee(\neg r\wedge s)$，所以 A 的析取范式为

$$\begin{aligned}
A&=((\neg p\vee(r\wedge\neg s)\vee(\neg r\wedge s))\wedge(\neg q\vee\neg r))\wedge(\neg r\vee\neg s)\\
&=((\neg p\wedge(\neg q\vee\neg r))\vee((r\wedge\neg s)\wedge(\neg q\vee\neg r))\\
&\quad\vee((\neg r\wedge s)\wedge(\neg q\vee\neg r)))\wedge(\neg r\vee\neg s)\\
&=((\neg p\wedge\neg q)\vee(\neg p\wedge\neg r)\vee(r\wedge\neg s\wedge\neg q)\vee(r\wedge\neg s\wedge\neg r)\\
&\quad\vee(\neg r\wedge s\wedge\neg q)\vee(\neg r\wedge s\wedge\neg r))\wedge(\neg r\vee\neg s)\\
&=(((\neg p\wedge\neg q)\vee(\neg p\wedge\neg r)\vee(r\wedge\neg s\wedge\neg q)\\
&\quad\vee(\neg r\wedge s\wedge\neg q)\vee(\neg r\wedge s))\wedge\neg r)\\
&\quad\vee(((\neg p\wedge\neg q)\vee(\neg p\wedge\neg r)\vee(r\wedge\neg s\wedge\neg q)\\
&\quad\vee(\neg r\wedge s\wedge\neg q)\vee(\neg r\wedge s))\wedge\neg s)\\
&=(\neg p\wedge\neg q\wedge\neg r)\vee(\neg p\wedge\neg r)\vee(\neg q\wedge\neg r\wedge s)\vee(\neg r\wedge s)\\
&\quad\vee(\neg p\wedge\neg q\wedge\neg s)\vee(\neg p\wedge\neg r\wedge\neg s)\vee(\neg q\wedge r\wedge\neg s)\\
&\overset{\text{吸收律}}{=\!=\!=}(\neg p\wedge\neg r)\vee(\neg r\wedge s)\vee(\neg p\wedge\neg q\wedge\neg s)\\
&\quad\vee(\neg p\wedge\neg r\wedge\neg s)\vee(\neg q\wedge r\wedge\neg s)
\end{aligned}$$

在上述析取范式中，第 1 个合取式 $\neg p\wedge\neg r$ 为 1 表示 p,r 都不去，所以 q,s 去；第 2 个合取式 $\neg r\wedge s$ 为 1 表示 r 不去，s 要去，于是有两种可能：p,s 或 q,s 去；第 3 个合取式 $\neg p\wedge\neg q\wedge\neg s$ 为 1 表示 p,q,s 都不去，不符合题意；同样，第 4 个合取式 $\neg p\wedge\neg r\wedge\neg s$ 为 1 表示 p,r,s 都不去，也不符合题意；第 5 个合取式 $\neg q\wedge r\wedge\neg s$ 为 1 表示 q,s 不去，r 去，于是 p,r 去.

综上所述，满足所给 3 个条件的选派方法为：(1) p,s 去；(2) q,s 去；(3) p,r 去.

3.5.2 命题公式的主析取范式及主合取范式

一般来说，一个命题公式的析取范式及合取范式不是唯一的. 例如，$A=(p\wedge q)\vee(p\wedge\neg q)=p$ 都是 A 的析取范式. 这种不唯一给有些问题的讨论带来不便. 下面根据命题公式中的所有命题变元，讨论给定命题公式的唯一的标准形式：主析取范式以及主合取范式.

给定命题公式 A，为了与后继课程有关内容紧密联系，从 A 中命题变元产生的极小项和极大项的角度来讨论 A 的主析取范式及主合取范式，在逻辑电路中也会讨论其相应的标准形式.

1. 主析取范式

【定义 3-7】 对于给定的命题变元，若由命题变元或其否定组成的合取式满足 (1) 每个命题变元或其否定两者之一只出现一次；(2) 按字典顺序或按下标从小到大顺序出现，称这

样的合取式为由所给命题变元产生的**极小项**(minimal term).

例如,两个命题变元 p 和 q 产生的极小项有

$$p \wedge q, p \wedge \neg q, \neg p \wedge q, \neg p \wedge \neg q$$

由 3 个命题变元 p,q 和 r 产生的极小项有

$$p \wedge q \wedge r, p \wedge q \wedge \neg r, p \wedge \neg q \wedge r, p \wedge \neg q \wedge \neg r,$$
$$\neg p \wedge q \wedge r, \neg p \wedge q \wedge \neg r, \neg p \wedge \neg q \wedge r, \neg p \wedge \neg q \wedge \neg r$$

对于每一个极小项只有一种指派使其取 1,例如极小项 $p \wedge \neg q \wedge \neg r$ 只有指派 $(p,q,r)=(1,0,0)$ 使其为 1.

可以根据这个结论对极小项编码.极小项用 m_i 表示,其下标 i 是由成真指派得到的二进制数或对应的十进制数,对于极小项 $p \wedge q \wedge \neg r$,成真指派得到的二进制数为 110,因为 $(110)_2=6$,所以 $p \wedge q \wedge \neg r = m_{110} = m_6$.

实际上,极小项的下标采用二进制记号更方便.

表 3-12 是由 3 个命题变元 p,q 和 r 产生的极小项及其成真指派和极小项的符号表示.

表 3-12

极 小 项	成真指派	极小项的符号表示 m_i	极 小 项	成真指派	极小项的符号表示 m_i
$p \wedge q \wedge r$	111	$m_{111}=m_7$	$\neg p \wedge q \wedge r$	011	$m_{011}=m_3$
$p \wedge q \wedge \neg r$	110	$m_{110}=m_6$	$\neg p \wedge q \wedge \neg r$	010	$m_{010}=m_2$
$p \wedge \neg q \wedge r$	101	$m_{101}=m_5$	$\neg p \wedge \neg q \wedge r$	001	$m_{001}=m_1$
$p \wedge \neg q \wedge \neg r$	100	$m_{100}=m_4$	$\neg p \wedge \neg q \wedge \neg r$	000	$m_{000}=m_0$

【定义 3-8】 对于命题公式 A,若 A 等值于由 A 中所有命题变元产生的若干个极小项的析取,则把后者称为 A 的**主析取范式**(major disjunctive form).

首先注意到,若命题公式 $A=A(p_1,p_2,\cdots,p_n)$,"若干个"最大为 2^n,最小为 0.很显然,所有极小项的析取为永真式 1,而 0 个极小项的析取意味着 A 为永假式 0,这时 A 的主析取范式不存在.除这两种极端情形外,A 均为中性式.

命题公式的主析取范式是析取范式,而一般来说,析取范式不是主析取范式.例如,例 3-17 中的 $A=(p \to q) \leftrightarrow r$,其析取范式为

$$A = (p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge r) \vee (q \wedge r)$$

它就不是 A 的主析取范式,主要原因是在该析取范式中,合取式 $\neg p \wedge r$ 以及 $q \wedge r$ 不是由 A 中 3 个命题 p,q,r 产生的极小项.但是可以在析取范式的基础上,对于合取式 $\neg p \wedge r$ 以及 $q \wedge r$,通过补充所缺少的命题变元将其转化为几个极小项的析取,即

$$q \wedge r = (p \vee \neg p) \wedge q \wedge r = (p \wedge q \wedge r) \vee (\neg p \wedge q \wedge r)$$
$$\neg p \wedge r = \neg p \wedge (q \vee \neg q) \wedge r = (\neg p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge r)$$

根据这个分析,可以得到求 A 的主析取范式的第一种方法:**等值演算法**.

利用等值演算法求 A 的主析取范式的计算步骤为:

(1) 求出 A 的析取范式;

(2) 利用分配律补充所缺少的命题变元.

【例 3-19】 设 p,q 和 r 是命题变元,求命题公式 $A=(p\to q)\leftrightarrow r$ 的主析取范式.

解 由例 3-17 知,A 的析取范式为

$$A=(p\wedge\neg q\wedge\neg r)\vee(\neg p\wedge r)\vee(q\wedge r)$$

因为

$$q\wedge r=(p\vee\neg p)\wedge q\wedge r=(p\wedge q\wedge r)\vee(\neg p\wedge q\wedge r)$$

$$\neg p\wedge r=\neg p\wedge(q\vee\neg q)\wedge r=(\neg p\wedge q\wedge r)\vee(\neg p\wedge\neg q\wedge r)$$

所以 A 的主析取范式为

$$\begin{aligned}A&=(p\wedge\neg q\wedge\neg r)\vee(\neg p\wedge q\wedge r)\vee(\neg p\wedge\neg q\wedge r)\vee(p\wedge q\wedge r)\vee(\neg p\wedge q\wedge r)\\&=(p\wedge\neg q\wedge\neg r)\vee(\neg p\wedge q\wedge r)\vee(\neg p\wedge\neg q\wedge r)\vee(p\wedge q\wedge r)\end{aligned}$$

由上面的主析取范式可知,使 A 取 1 的真值指派为

$$(p,q,r)=(1,0,0),(0,1,1),(0,0,1),(1,1,1)$$

实际上,可以利用 A 的真值表求 A 的主析取范式.

下面介绍求主析取范式的第二种方法:**真值表法**.

利用真值表求主析取范式的 3 个步骤如下.

(1) 写出命题公式 A 的真值表.

(2) 对于使 A 取 1 的指派,写出对应的极小项,使该极小项在该指派下也为 1.

例如,若$(p,q,r)=(1,1,1)$使 A 取 1,则对应的极小项为 $m_{111}=m_7=p\wedge q\wedge r$;

若$(p,q,r)=(1,0,0)$使 A 取 1,则对应的极小项为 $m_{100}=m_4=p\wedge\neg q\wedge\neg r$;

若$(p,q,r)=(0,0,0)$使 A 取 1,则对应的极小项为 $m_{000}=m_0=\neg p\wedge\neg q\wedge\neg r$.

(3) (可以证明)A 等值于所有这样写出的极小项的析取.

【例 3-20】 设 p,q 和 r 是命题变元,求命题公式 $A=(p\vee q)\to r$ 的主析取范式.

解 命题公式 $A=(p\vee q)\to r$ 的真值表如表 3-13 所示.

使 $A=(p\vee q)\to r$ 取 1 的指派 111,101,011,001,000 对应的极小项分别为 $p\wedge q\wedge r$, $p\wedge\neg q\wedge r$, $\neg p\wedge q\wedge r$, $\neg p\wedge\neg q\wedge r$, $\neg p\wedge\neg q\wedge\neg r$. 于是有

$$\begin{aligned}A=&(p\wedge q\wedge r)\vee(p\wedge\neg q\wedge r)\vee(\neg p\wedge q\wedge r)\vee(\neg p\wedge\neg q\wedge r)\\&\vee(\neg p\wedge\neg q\wedge\neg r)\end{aligned}$$

表 3-13

p	q	r	$p\vee q$	$(p\vee q)\to r$	p	q	r	$p\vee q$	$(p\vee q)\to r$
1	1	1	1	1	0	1	1	1	1
1	1	0	1	0	0	1	0	1	0
1	0	1	1	1	0	0	1	0	1
1	0	0	1	0	0	0	0	0	1

结合上面的例子,根据等值式的定义容易得出:A 等值于所有这样写出的极小项的析取.

2. 主合取范式

主合取范式的讨论与主析取范式是完全类似的,为了方便自学,还是进行完整的讨论.

【定义 3-9】 对于给定的命题变元,若由命题变元或其否定组成的析取式满足:

(1) 每个命题变元或其否定两者之一只出现一次;

(2) 按字典顺序或按下标从小到大顺序出现,称这样的析取式为由所给命题变元产生的**极大项**(maximal term).

例如,两个命题变元 p 和 q 产生的极大项有

$$p \vee q, p \vee \neg q, \neg p \vee q, \neg p \vee \neg q$$

由 3 个命题变元 p,q 和 r 产生的极大项有

$$p \vee q \vee r, p \vee q \vee \neg r, p \vee \neg q \vee r, p \vee \neg q \vee \neg r,$$
$$\neg p \vee q \vee r, \neg p \vee q \vee \neg r, \neg p \vee \neg q \vee r, \neg p \vee \neg q \vee \neg r$$

对于每一个极大项只有一种指派使其取 0,例如极大项 $p \vee \neg q \vee \neg r$ 只有指派 $(p,q,r)=(0,1,1)$ 使其为 0.

可以根据这个结论对极大项编码.极大项用 M_i 表示,其下标 i 是由成假指派得到的二进制数或对应的十进制数,对于极大项 $p \vee \neg q \vee \neg r$,成假指派得到的二进制数为 011,因为 $(011)_2=3$,所以 $p \vee \neg q \vee \neg r = M_{011} = M_3$.

同样,极大项的下标采用二进制记号更方便.

表 3-14 是由 3 个命题变元 p,q 和 r 产生的极大项及其成假指派和极大项的符号表示.

表 3-14

极大项	成假指派	极大项的符号表示 M_i	极大项	成假指派	极大项的符号表示 M_i
$p \vee q \vee r$	000	$M_{000}=M_0$	$\neg p \vee q \vee r$	100	$M_{100}=M_4$
$p \vee q \vee \neg r$	001	$M_{001}=M_1$	$\neg p \vee q \vee \neg r$	101	$M_{101}=M_5$
$p \vee \neg q \vee r$	010	$M_{010}=M_2$	$\neg p \vee \neg q \vee r$	110	$M_{110}=M_6$
$p \vee \neg q \vee \neg r$	011	$M_{011}=M_3$	$\neg p \vee \neg q \vee \neg r$	111	$M_{111}=M_7$

显然,有 $\neg M_i = m_i$.

【定义 3-10】 对于命题公式 A,若 A 等值于由 A 中所有命题变元产生的若干个极大项的合取,则把后者称为 A 的**主合取范式**(major conjunctive form).

首先注意到,若命题公式 $A=A(p_1,p_2,\cdots,p_n)$,“若干个”最大数为 2^n,最小数为 0.很显然,所有极大项的合取为永假式 0,而 0 个极大项的合取意味着 A 为永真式 1,这时 A 的主合取范式不存在.除这两种极端情形外,A 均为中性公式.

命题公式的主合取范式是合取范式,而一般来说,合取范式不是主合取范式.例如,例 3-17 中的 $A=(p \to q) \leftrightarrow r$,其合取范式为

$$A=(p \vee r) \wedge (\neg q \vee r) \wedge (\neg p \vee q \vee \neg r)$$

它就不是 A 的主合取范式,主要原因是在该合取范式中,析取式 $p \vee r$ 以及 $\neg q \vee r$ 不是由 A 中 3 个命题 p,q,r 产生的极大项.但是可以在合取范式的基础上,对于析取式 $p \vee r$ 以及 $\neg q \vee r$,通过补充所缺少的命题变元将其转化为几个最大项的合取.

$$p \vee r = p \vee (q \wedge \neg q) \vee r = (p \vee q \vee r) \wedge (p \vee \neg q \vee r)$$
$$\neg q \vee r = (p \wedge \neg p) \vee \neg q \vee r = (p \vee \neg q \vee r) \wedge (\neg p \vee \neg q \vee r)$$

根据这个分析，得到求 A 的主合取范式的第一种方法：**等值演算法**.

利用等值演算法求 A 的主合取范式的计算步骤为：

(1) 求出 A 的合取范式；

(2) 利用分配律补充所缺少的命题变元.

【例 3-21】 设 p,q 和 r 是命题变元，求命题公式 $A=(p\to q)\leftrightarrow r$ 的主合取范式.

解 由例 3-17 知，A 的合取范式为

$$A=(p\vee r)\wedge(\neg q\vee r)\wedge(\neg p\vee q\vee\neg r)$$

因为

$$p\vee r=p\vee(q\wedge\neg q)\vee r=(p\vee q\vee r)\wedge(p\vee\neg q\vee r)$$

$$\neg q\vee r=(p\wedge\neg p)\vee\neg q\vee r=(p\vee\neg q\vee r)\wedge(\neg p\vee\neg q\vee r)$$

所以 A 的主合取范式为

$$\begin{aligned}A&=(p\vee q\vee r)\wedge(p\vee\neg q\vee r)\wedge(p\vee\neg q\vee r)\\&\quad\wedge(\neg p\vee\neg q\vee r)\wedge(\neg p\vee q\vee\neg r)\\&=(p\vee q\vee r)\wedge(p\vee\neg q\vee r)\wedge(\neg p\vee\neg q\vee r)\wedge(\neg p\vee q\vee\neg r)\end{aligned}$$

由上面的主合取范式可知，使 A 取 0 的真值指派为

$$(p,q,r)=(0,0,0),(0,1,0),(1,1,0),(1,0,1)$$

实际上，可以利用 A 的真值表求 A 的主合取范式.

下面介绍求 A 的主合取范式的第 2 种方法：**真值表法**.

利用真值表法求 A 的主合取范式的 3 个计算步骤为：

(1) 写出命题公式 A 的真值表.

(2) 对于使 A 取 0 的指派，写出对应的极大项，使该极大项在该指派下也为 0.

例如，若 $(p,q,r)=(1,1,1)$ 使 A 取 0，则对应的极大项为 $M_{111}=M_7=\neg p\vee\neg q\vee\neg r$；

若 $(p,q,r)=(1,0,0)$ 使 A 取 0，则对应的极大项为 $M_{100}=M_4=\neg p\vee q\vee r$；

若 $(p,q,r)=(0,0,0)$ 使 A 取 0，则对应的极大项为 $M_{000}=M_0=p\vee q\vee r$.

(3) (可以证明) A 等值于所有这样写出的极大项的合取.

【例 3-22】 设 p,q 和 r 是命题变元，求命题公式 $A=(p\vee q)\to r$ 的主合取范式.

解 命题公式 $A=(p\vee q)\to r$ 的真值表见表 3-16.

使 $A=(p\vee q)\to r$ 取 0 的指派 110，100，010 对应的极大项分别为 $\neg p\vee\neg q\vee r$，$\neg p\vee q\vee r$，$p\vee\neg q\vee r$. 于是有

$$A=(\neg p\vee\neg q\vee r)\wedge(\neg p\vee q\vee r)\wedge(p\vee\neg q\vee r)$$

结合上面的例子，根据等值式的定义可以证明：A 等值于所有这样写出的极大项的合取.

由上面的讨论有以下定理.

【定理 3-9】 任意非永假(非永真)命题公式都存在唯一的主析取范式(主合取范式).

显然，命题公式的主析取范式和主合取范式是等值的. 主析取范式中所含的极小项个数加上主合取范式中所含的极大项个数等于该命题公式的真值指派数目. 进一步，可以从主析取范式求出主合取范式，反过来亦然.

利用命题公式的主析取范式及主合取范式判定其类型. 由例 3-19 或例 3-21 知，命题公式 $A=(p\to q)\leftrightarrow r$ 是中性公式. 再看一个简单的例子.

【例 3-23】 设 p 和 q 是命题变元，利用主范式判断命题公式 $p\wedge(p\rightarrow\neg q)$ 的类型.

解 $p\wedge(p\rightarrow\neg q)=p\wedge(\neg p\vee\neg q)=(p\wedge\neg p)\vee(p\wedge\neg q)=p\wedge\neg q$，显然所给命题公式的主析取范式中仅含一个极小项，所以它是中性公式.

利用命题公式的主析取范式及主合取范式可以判断两个命题公式是否等值.

【例 3-24】 利用主范式判断下述两个命题公式是否等值.

(1) $p\rightarrow(q\rightarrow r)$.

(2) $(p\vee q)\rightarrow r$.

解 (1) $p\rightarrow(q\rightarrow r)=p\rightarrow(\neg q\vee r)=\neg p\vee\neg q\vee r$.

(2) $(p\vee q)\rightarrow r=\neg(p\vee q)\vee r=(\neg p\wedge\neg q)\vee r=(\neg p\vee r)\wedge(\neg q\vee r)$

$$=(\neg p\vee(q\wedge\neg q)\vee r)\wedge((p\wedge\neg p)\vee\neg q\vee r)$$

$$=(\neg p\vee q\vee r)\wedge(\neg p\vee\neg q\vee r)\wedge(p\vee\neg q\vee r)\wedge(\neg p\vee\neg q\vee r)$$

$$=(\neg p\vee q\vee r)\wedge(\neg p\vee\neg q\vee r)\wedge(p\vee\neg q\vee r).$$

命题公式 $p\rightarrow(q\rightarrow r)$ 的主合取范式中，仅一个极大项；命题公式 $(p\vee q)\rightarrow r$ 的主合取范式中，有 3 个极大项. 于是得出，所给的两个命题公式不等值.

下面的例子说明，命题公式的主析取范式及主合取范式是如何应用在数字逻辑等后继课程中的.

【例 3-25】 设命题公式 A 的真值表如表 3-15 所示，求 A.

表 3-15

p	q	r	A	p	q	r	A
1	1	1	1	0	1	1	0
1	1	0	0	0	1	0	0
1	0	1	0	0	0	1	0
1	0	0	1	0	0	0	1

解法 1 因为 A 等值于所有使 A 取 1 的指派对应的极小项的析取，所以

$$A=(p\wedge q\wedge r)\vee(p\wedge\neg q\wedge\neg r)\vee(\neg p\wedge\neg q\wedge\neg r)$$

解法 2 因为 A 等值于所有使 A 取 0 的指派对应的极大项的合取，所以

$$A=(\neg p\vee\neg q\vee r)\wedge(\neg p\vee q\vee\neg r)\wedge(p\vee\neg q\vee\neg r)\wedge(p\vee\neg q\vee r)\wedge(p\vee q\vee\neg r)$$

在上例中，解法 1 比解法 2 好，因为极小项的个数为 3 而极大项的个数为 5，所以在电路实现时对 A 进行的化简要容易些.

一般原则是，若 A 取 1 的个数小于取 0 的个数，求出主析取范式；若 A 取 0 的个数小于取 1 的个数，求出主合取范式. 不过，再次提醒注意，同一个命题公式的主析取范式与其主合取范式是等值的.

从例 3-25 可知，只要给出了一个命题公式 A 的真值表，就可以将该命题公式 A（的表达式）求出来. 这一点在 3.6 节中也会用到.

另外，根据真值表法可知，若得出了命题公式 A 的主析取范式，则可以得出使 A 为真的所有指派，进而得出使 A 为假的所有指派，因此可以得出命题公式 A 的主合取范式；反过来亦然.

习 题 3.5

1. 求下列命题公式的析取范式与合取范式.

(1) $p \land (p \to q)$.

(2) $\neg (p \land q) \land (p \lor q)$.

(3) $(\neg p \land q) \to r$.

(4) $(p \to q) \to r$.

2. 在一次研讨会上,3 名与会者根据王教授的口音分别作出下述判断.

甲说:“王教授不是苏州人,是上海人”.

乙说:“王教授不是上海人,是苏州人”.

丙说:“王教授不是杭州人,也不是上海人”.

王教授听后笑道:“你们 3 人中有一个人全说对了,有一个人全说错了,有一个人对错各半.”请问王教授是哪里人?

3. 当 p,q,r,s 4 人考试成绩出来后,有人问 4 人中谁的成绩最好. p 说“不是我”,q 说“是 s”,r 说“是 q”,s 说“不是我”. 4 人的回答只有一个人符合实际,问哪一位的成绩最好. 若有 2 人成绩并列最好,应是哪两位?

4. 已知 p,q,r,s 这 4 个人中有且仅有两个人参加围棋比赛,但必须满足下列 4 个条件:

(1) p 和 q 仅一个人参加;

(2) 若 r 参加,则 s 也参加;

(3) q 和 s 至多参加一个人;

(4) 若 s 不参加,则 p 也不参加.

应派哪两个人去参加比赛?

5. 分别用等值演算法和真值表法,求下列命题公式的主析取范式及主合取范式,并判断其类型.

(1) $(\neg p \lor \neg q) \to (p \leftrightarrow \neg q)$.

(2) $(q \to p) \land (\neg p \land q)$.

(3) $(q \lor \neg p) \to r$.

(4) $(p \to (q \land r)) \land (\neg p \to (\neg q \land \neg r))$.

6. 利用主范式判断命题公式$(p \to q) \lor (q \to r) \to ((p \lor q) \to r)$的类型.

7. 利用主范式判断下列两个命题公式是否等值:

(1) $(p \land q) \lor (\neg p \land r) \lor (q \land r)$;

(2) $(p \land q) \lor (\neg p \land r)$.

8. 设某命题公式 A 的真值表为表 3-16,求 A.

表 3-16

p	q	r	A	p	q	r	A
1	1	1	0	0	1	1	1
1	1	0	0	0	1	0	1
1	0	1	1	0	0	1	0
1	0	0	0	0	0	0	0

9. 设计一盏电灯的开关电路时，要求受 3 个开关 A，B，C 的控制：当且仅当 A，C 同时关闭或 B，C 同时关闭时灯亮. 用 F 表示灯亮，p，q，r 分别表示开关 A，B，C 关闭，求 $F=F(p,q,r)$ 的逻辑表达式以及 F 的主析取范式及主合取范式.

10. 某电路中有一只灯泡和 3 个开关 A，B，C. 已知当且仅当在下述 4 种情况之一灯亮：

(1) C 的搬键向上，A 和 B 的搬键向下；

(2) A 的搬键向上，B 和 C 的搬键向下；

(3) B 和 C 的搬键向上，A 的搬键向下；

(4) A 和 B 的搬键向上，C 的搬键向下.

令 F 表示灯亮，p，q，r 分别表示 A，B，C 的搬键向上，求 $F=F(p,q,r)$ 的逻辑表达式以及 F 的主合取范式.

3.6 联结词集合的功能完备性

在 3.2 节中介绍了 9 个联结词，联结词一共有多少个，同时哪些联结词集合具有功能完备性？这些内容可以从一定的理论高度帮助理解逻辑门电路的种类及其按一定要求化简逻辑函数等问题.

3.6.1 联结词的个数

考虑含两个命题变元 p 和 q 的情形. 由 p 和 q 可构成不等值的命题公式共 $2^{2^2}=16$ 个，记为 $A_i(i=1,2,\cdots,16)$，见表 3-17.

表 3-17

p	q	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}	A_{14}	A_{15}	A_{16}
1	1	1	0	1	1	0	0	1	0	1	0	1	0	1	0	1	0
1	0	1	0	1	0	0	1	0	1	1	0	0	1	0	1	1	0
0	1	1	0	0	1	1	0	0	1	1	0	1	0	0	1	0	1
0	0	1	0	0	0	1	1	0	1	0	1	1	0	1	0	1	0

由等值式的定义可知，$A_1=1$，$A_2=0$，$A_3=p$，$A_4=q$，$A_5=\neg p$，$A_6=\neg q$，$A_7=p\wedge q$，$A_8=p\uparrow q$，$A_9=p\vee q$，$A_{10}=p\downarrow q$，$A_{11}=p\rightarrow q$，$A_{12}=p\overset{n}{\rightarrow}q$，$A_{13}=p\leftrightarrow q$，$A_{14}=p\oplus q$，$A_{15}=q\rightarrow p$，$A_{16}=q\overset{n}{\rightarrow}p$.

除 $A_1=1$，$A_2=0$，$A_3=p$，$A_4=q$ 以及重复的联结词(A_5 与 A_6、A_{11} 与 A_{15}、A_{12} 与 A_{16})外，逻辑联结词共 9 个：1 元联结词 1 个，2 元联结词 8 个.

在 3.4 节曾提到，集合运算与逻辑运算之间有非常紧密的联系，于是有下述问题供大家思考.

问题 1 能否类似于真值表形式给出集合运算的定义？若能，如何给出？

前面已经说明了，不同的 1 元和 2 元逻辑运算共 9 种(3 元逻辑运算更多)，而集合运算只介绍了 5 种.

问题 2 给出另外 4 种集合运算的定义.

问题 3　9 种逻辑运算与 9 种集合运算是如何对应的?

3.6.2　功能完备联结词集

实际上,有些逻辑运算可以借助于其他联结词加以定义,在 3.4 节中已经看到了这一点.很快就可以知道,有些联结词如 $\neg$ 就不能由 $\wedge$ 和 $\vee$ 加以定义,这涉及联结词集合的功能完备性.

【定义 3-11】　对于若干个联结词组成的非空集合 S,若任意的命题公式都可由仅含 S 中的联结词等值地表示出来,则称 S 为**功能完备联结词集**(complete group of connectives, adequate set of connectives).

将 S 中的联结词理解为门电路,则 S 是功能完备的是指任何的逻辑电路都可以由这些门电路实现.

由 3.5 节定理 3-9 知,任意的命题公式都存在唯一的主析取范式或主合取范式,于是,任意的命题公式都可以由 $\{\neg, \wedge, \vee\}$ 中的联结词等值表示出来,因此,有以下定理:

【定理 3-10】　$\{\neg, \wedge, \vee\}$ 是功能完备联结词集.

推论　以下联结词集都是功能完备的.

(1) $\{\downarrow\}$.

(2) $\{\uparrow\}$.

(3) $\{\neg, \wedge\}$.

(4) $\{\neg, \vee\}$.

(5) $\{\neg, \rightarrow\}$.

证　只证(2)和(4),其余留作练习.

(2) 根据定理 3-10,只需证明:$\neg p, p\wedge q, p\vee q$ 可由仅含“$\uparrow$”的命题公式等值表示.

因为

$$\neg p = \neg(p \wedge p) = p \uparrow p,$$
$$p \wedge q = \neg(\neg(p \wedge q)) = \neg(p \uparrow q) = (p \uparrow q) \uparrow (p \uparrow q),$$
$$p \vee q = \neg(\neg p \wedge \neg q) = (\neg p) \uparrow (\neg q) = (p \uparrow p) \uparrow (q \uparrow q)$$

所以,$\{\uparrow\}$ 是功能完备联结词集.

(4) 只需证明:$p\wedge q$ 可由仅含 $\{\neg, \vee\}$ 的命题公式等值表示.

因为 $p\wedge q = \neg(\neg p \vee \neg q)$,由定理 3-10 知 $\{\neg, \vee\}$ 是功能完备联结词集.

【例 3-26】　定义 3 元联结词 f 如表 3-18,证明:$\{f\}$ 是功能完备的.

表　3-18

p	q	r	$f(p,q,r)$	p	q	r	$f(p,q,r)$
1	1	1	0	0	1	1	0
1	1	0	1	0	1	0	0
1	0	1	1	0	0	1	1
1	0	0	1	0	0	0	1

证　由真值表 3-21,可得出 $f(p,q,r)$ 的主合取范式为

$$f(p,q,r) = (\neg p \vee \neg q \vee \neg r) \wedge (p \vee \neg q \vee \neg r) \wedge (p \vee \neg q \vee r)$$

于是,有 $f(p,p,p)=\neg p$ 且 $f(\neg p,\neg p,\neg q)=p \vee q$. 由推论(4)知,$\{\neg,\vee\}$是功能完备的,因此$\{f\}$是功能完备的.

【例 3-27】 化简命题公式$((p \vee q) \to r) \to p$,并用仅含联结词$\{\neg,\wedge\}$的等值的命题公式表示.

解

$$\begin{aligned}((p \vee q) \to r) \to p &= (\neg (p \vee q) \vee r) \to p \\ &= \neg(\neg(p \vee q) \vee r) \vee p \\ &= ((p \vee q) \wedge \neg r) \vee p \\ &= ((p \vee q) \vee p) \wedge (\neg r \vee p) \\ &= (p \vee q) \wedge (p \vee \neg r) \\ &= p \vee (q \wedge \neg r) \\ &= \neg(\neg p \wedge \neg(q \wedge \neg r))\end{aligned}$$

下面考虑不具有功能完备性的联结词集.

【例 3-28】 证明:$\{\wedge,\to\}$不是功能完备的联结词集.

证 首先证明,对于只含有联结词$\{\wedge,\to\}$的任意命题公式 A,在所有命题变元均取 1 时,A 的真值为 1.

对 A 中所含的联结词个数 n 使用第二数学归纳法.

当 $n=0$ 时,显然成立.

假设小于等于 n 时成立,当 A 含 $n+1$ 个联结词时,这时 $A=B \wedge C$ 或 $A=B \to C$,由归纳假设知,在所有命题变元均取 1 时,B 和 C 的真值为 1,进而 A 的真值为 1.

对于命题变元 p,由上面的讨论可知 $p \wedge \neg p$ 不能用仅含联结词$\{\wedge,\to\}$的命题公式等值表示,故$\{\wedge,\to\}$不是功能完备的联结词集.

【定义 3-12】 设 S 是功能完备的联结词集,而 S 的任意非空真子集都不是功能完备的联结词集,则称 S 为**极小的功能完备的联结词集**.

由于$\{\neg\}$,$\{\wedge\}$,$\{\vee\}$,$\{\to\}$不是功能完备的,所以由定理 3-10 的推论有:

【定理 3-11】 下列联结词集合是极小功能完备的.

(1) $\{\downarrow\}$.

(2) $\{\uparrow\}$.

(3) $\{\neg,\wedge\}$.

(4) $\{\neg,\vee\}$.

(5) $\{\neg,\to\}$.

人们通常先介绍 5 种逻辑运算 $\neg,\wedge,\vee,\to,\leftrightarrow$,在命题公式的定义中也只用这 5 种. 实际上,这 5 种逻辑运算是不全面的,还有 4 种. 若从功能完备的角度去看,又有多余的联结词.

知道了逻辑运算的个数以及极小的功能完备的联结词集,对于我们进一步学习、研究逻辑演算形式系统是有帮助的.

在实际应用中,联结词"$\uparrow$"以及"$\downarrow$"可推广到多个命题变元上去,如$\neg(p \wedge q \wedge r)$,$\neg(p \vee q \vee r \vee s)$等,也可以构造出组合门电路,如"与或非门"等.

习　题　3.6

1. 证明：通过考虑含一个命题变元 p 的不等值的命题公式，只能得出一个联结词 $\neg$.

2. 证明：含 n 个命题变元 $p_1,p_2,\cdots,p_n$ 的不等值的命题公式的个数为 2^{2^n}.

3. 证明：以下联结词集都是功能完备的.

(1) $\{\downarrow\}$.

(2) $\{\neg,\wedge\}$.

(3) $\{\neg,\rightarrow\}$.

4. 证明：下列联结词集都不是功能完备的联结词集.

(1) $\{\neg\}$.

(2) $\{\wedge\}$.

(3) $\{\vee\}$.

(4) $\{\rightarrow\}$.

5. 证明：下列联结词集都不是功能完备的联结词集.

(1) $\{\neg,\leftrightarrow\}$.

(2) $\{\neg,\oplus\}$.

(3) $\{\wedge,\vee\}$.

3.7　命题逻辑中的推理

逻辑学的主要内容是研究推理，推理是从一些前提推出结论的思维过程.实际问题中的推理，需要对前提做深入分析，才能得出结论，如由两直线平行，得出同位角相等以及由一元二次方程的判别式大于0得出方程有两个不相等的实数根等就是这样的一些推理.

数理逻辑主要是用数学的方法研究逻辑中的推理，它关心的是推理形式的有效性问题.

例如，下面两个不同的推理.

(1) 若两直线平行，则同位角相等.

这两直线是平行的，所以，同位角相等.

(2) 若两个三角形全等，则其对应边相等.

这两个三角形全等，所以，它们的对应边相等.

都具有如下的推理形式

$$由\ p\rightarrow q,p\ 得出\ q.$$

所谓推理形式的有效性是指，如果前提全为真，那么所得结论必然为真，而不考虑前提和结论的真实含义.有效的推理形式是四海皆准的推理规则.

3.7.1　推理形式有效性的定义

【定义 3-13】 设 $H_1,H_2,\cdots,H_n$ 和 C 是命题公式，若 $H_1,H_2,\cdots,H_n$ 全为真，可得出 C 必然真，则称由 $H_1,H_2,\cdots,H_n$ 得出 C 的**推理形式是有效的**(valid argument form)，记为 $H_1,H_2,\cdots,H_n\Rightarrow C$(或 $H_1,H_2,\cdots,H_n\ \models C$，通常在讨论形式系统的语义推理时使用，而

$H_1, H_2, \cdots, H_n \vdash C$ 在讨论语构推理时使用)，其中 $H_1, H_2, \cdots, H_n$ 称为**前提**(antecedent，premise，hypothesis)，C 称为**结论**(conclusion).

$H_1, H_2, \cdots, H_n \Rightarrow C$ 可简称 $H_1, H_2, \cdots, H_n$ **逻辑推出**(logically follows)或**逻辑蕴涵**(logically implies)C，“$\Rightarrow$”是“推出”符号，$H_1, H_2, \cdots, H_n \Rightarrow C$ 称为**推理规则**.

命题公式由 $H_1, H_2, \cdots, H_n$ 全为真，可得出 $H_1 \wedge H_2 \wedge \cdots \wedge H_n$ 为真. 于是，由 3.3 节例 3-10 的说明可知，由 $H_1, H_2, \cdots, H_n$ 全为真可得出 C 必然真的充要条件是 $H_1 \wedge H_2 \wedge \cdots \wedge H_n \rightarrow C$ 为永真式. 因此有

【定理 3-12】 设 $H_1, H_2, \cdots, H_n$ 和 C 是命题公式，则 $H_1, H_2, \cdots, H_n \Rightarrow C$ 的充要条件是 $H_1 \wedge H_2 \wedge \cdots \wedge H_n \rightarrow C$ 是永真式，即 $H_1 \wedge H_2 \wedge \cdots \wedge H_n \Rightarrow C$.

正因为这样，又称 $H_1, H_2, \cdots, H_n \Rightarrow C$ 是**永真蕴涵式**或**逻辑蕴涵式**. 因此，“$\Rightarrow$”又是“永真蕴涵”或“逻辑蕴涵”符号，它与蕴涵联结词“$\rightarrow$”是不同的.

注意 就两个命题公式来说，$\Rightarrow$ 是关系符号，$A \Rightarrow B$ 是逻辑蕴涵式，$\rightarrow$ 是运算符号，$A \rightarrow B$ 是命题公式，而通常所说的蕴涵指逻辑蕴涵.

定理 3-12 给出了等值式与永真蕴涵式之间的联系. 可以利用定理 3-12 去证明一些永真式，参见本节的习题第 10 题.

从推理的角度看，将 $A = B$ 写成 $A \Leftrightarrow B$ 更适合.

【定理 3-13】 设 A 和 B 是命题公式，则 $A \Leftrightarrow B$ 的充要条件是 $A \Rightarrow B$ 且 $B \Rightarrow A$.

证 利用 $A \leftrightarrow B = (A \rightarrow B) \wedge (B \rightarrow A)$ 即得.

在实际推理中，特别是数学证明，上述定理 3-13 很常用.

可以证明，命题公式间的永真蕴涵关系是偏序关系.

【定理 3-14】 设 A，B 和 C 是命题公式，下述结论成立.

(1) $A \Rightarrow A$(自反性).

(2) 若 $A \Rightarrow B$ 且 $B \Rightarrow A$，则 $A = B$(反对称性).

(3) 若 $A \Rightarrow B$ 且 $B \Rightarrow C$，则 $A \Rightarrow C$(传递性).

证 (1) 显然.

(2) 由定理 3-13 即得.

(3) 因为 $A \Rightarrow B$ 且 $B \Rightarrow C$，所以 $A \rightarrow B$ 且 $B \rightarrow C$ 永真，由此可以推出：若 A 真则 C 真，于是 $A \rightarrow C$ 永真，因此有 $A \Rightarrow C$.

根据定理 3-12 可得出命题公式间的永真蕴涵关系 $\Rightarrow$ 还具有下面两条性质.

【定理 3-15】 设 A，B 和 C 是命题公式，下述结论成立.

(1) 若 $A \Rightarrow C$ 且 $B \Rightarrow C$，则 $A \vee B \Rightarrow C$.

(2) 若 $C \Rightarrow A$ 且 $C \Rightarrow B$，则 $C \Rightarrow A \wedge B$.

证 (1) 因为 $A \Rightarrow C$ 且 $B \Rightarrow C$，所以 $A \rightarrow C$ 且 $B \rightarrow C$ 永真，于是由 $A \vee B$ 真有 C 真，因此 $A \vee B \rightarrow C$ 永真，进而 $A \vee B \Rightarrow C$.

(2) 因为 $C \Rightarrow A$ 且 $C \Rightarrow B$，所以 $C \rightarrow A$ 且 $C \rightarrow B$ 永真，于是由 C 真有 $A \wedge B$ 真，因此 $C \rightarrow A \wedge B$ 永真，进而 $C \Rightarrow A \wedge B$.

由定理 3-15 可以得出以下定理.

【定理 3-16】 设 A，B 是命题公式，则对于命题公式间的永真蕴涵关系 $\Rightarrow$，

(1) $\sup \{A, B\} = A \vee B$.

(2) $\inf \{A, B\} = A \wedge B$.

证 （1）显然，$A\rightarrow(A\vee B)$永真，于是 $A\Rightarrow A\vee B$. 同理有 $B\Rightarrow A\vee B$. 所以，$A\vee B$ 是 A 和 B 的上界. 假设 C 是 A 和 B 的任意上界，即 $A\Rightarrow C$ 且 $B\Rightarrow C$，由定理 3-14 知，$A\vee B\Rightarrow C$. 因此，$A\vee B$ 是 A 和 B 的最小上界，进而有 $\sup\{A,B\}=A\vee B$.

（2）（留作练习）.

3.7.2 基本推理规则

下面举例说明，证明推理形式有效性的 4 种方法.

【例 3-29】 设 A 和 B 是命题公式，证明：$A\rightarrow B, A\Rightarrow B$.

分析 根据定义，只需证明$((A\rightarrow B)\wedge A)\rightarrow B$ 永真. 由永真式的代入定理知，只需证明：对于命题变元 p,q，有$((p\rightarrow q)\wedge p)\rightarrow q$ 永真.

证法 1 真值表法. 写出命题公式$((p\rightarrow q)\wedge p)\rightarrow q$ 的真值表见表 3-19.

显然，$((p\rightarrow q)\wedge p)\rightarrow q$ 永真.

证法 2 取值法. 假设$(p\rightarrow q)\wedge p$ 取真，则 $p\rightarrow q$ 及 p 均取真，进而 q 为真，因此$((p\rightarrow q)\wedge p)\rightarrow q$ 永真.

表 3-19

p	q	$p\rightarrow q$	$(p\rightarrow q)\wedge p$	$((p\rightarrow q)\wedge p)\rightarrow q$	p	q	$p\rightarrow q$	$(p\rightarrow q)\wedge p$	$((p\rightarrow q)\wedge p)\rightarrow q$
1	1	1	1	1	0	1	1	0	1
1	0	0	0	1	0	0	1	0	1

证法 3 等值演算法.

$$\begin{aligned}((p\rightarrow q)\wedge p)\rightarrow q &= ((\neg p\vee q)\wedge p)\rightarrow q\\ &= ((\neg p\wedge p)\vee(p\wedge q))\rightarrow q = (p\wedge q)\rightarrow q = \neg(p\wedge q)\vee q\\ &= (\neg p\vee\neg q)\vee q = \neg p\vee(\neg q\vee q) = \neg p\vee 1 = 1\end{aligned}$$

证法 4 主范式法.

$((p\rightarrow q)\wedge p)\rightarrow q$ 的主析取范式和主合取范式分别为：

$((p\rightarrow q)\wedge p)\rightarrow q = (p\wedge q)\vee(p\wedge\neg q)\vee(\neg p\wedge q)\vee(\neg p\wedge\neg q)$

$((p\rightarrow q)\wedge p)\rightarrow q$（主合取范式不存在）

从主范式都可以得出$((p\rightarrow q)\wedge p)\rightarrow q$ 永真.

类似地可以证明下列基本推理规则.

设 A，B 和 C 是命题公式，如表 3-20 所示为基本推理规则或永真蕴涵式，要求记住.

表 3-20 基本逻辑蕴涵式 Ⅰ

(1) $A\wedge B\Rightarrow A$，$A\wedge B\Rightarrow B$(**化简**).

(2) $A\Rightarrow A\vee B$，$B\Rightarrow A\vee B$(**附加**).

(3) $A,B\Rightarrow A\wedge B$(**合取引入**).

(4) $A\vee B,\neg A\Rightarrow B$(**析取三段论**).

(5) $A\rightarrow B,A\Rightarrow B$(**假言推理**).

(6) $A\rightarrow B,\neg B\Rightarrow\neg A$(**拒取式**).

(7) $A\rightarrow B,B\rightarrow C\Rightarrow A\rightarrow C$(**假言三段论**).

(8) $A\vee B,A\rightarrow C,B\rightarrow C\Rightarrow C$(**二难推理**).

3.7.3 命题逻辑的自然推理系统

自然推理的构造法是判定推理形式有效性的又一种方法，它主要是为今后进一步学习数理逻辑，尤其是为逻辑的公理化推理系统做准备的. 自然推理的基本思想是，确定一些推理规则，然后根据这些推理规则从前提出发，把结论推出来. 自然推理系统是德国逻辑学家 G. Gentzen和波兰逻辑学家 S. Jaskowski 在 1934 年独立给出的演绎逻辑系统的一个创新成果.

作为推理系统，原则上有以下 4 个部分.

(1) 它应有初始符号，它是系统中允许出现的字符. 自然推理系统的初始符号有以下 3 类.

① 命题变元 $p,q,\cdots,r,\cdots,p_i,q_i,r_i,\cdots$.

② 5 个联结词 $\neg,\wedge,\vee,\rightarrow,\leftrightarrow$.

因为这 5 个联结词足以对实际问题进行描述了. 若出现异或等其他联结词情形，则要求归约到这 5 个联结词，这是容易办到的.

③ 左右圆括号："(","）".

(2) 定义推理系统中的公式，它是按一定的形成规则得到的有意义的符号串. 粗略地说，它就是命题公式，但它原则上不出现除 $\neg,\wedge,\vee,\rightarrow,\leftrightarrow$ 外的其他联结词，同时原则上不出现命题常量 1 和 0.

(3) 确定公理，就是推理系统中不加推导就承认的公式. 从语义的角度看，它就是永真式. 自然推理系统中没有公理，这一点是与公理推理系统截然不同的.

(4) 确定推理规则. 在自然推理系统中，把所有与 5 个联结词 $\neg,\wedge,\vee,\rightarrow,\leftrightarrow$ 有关的基本逻辑蕴涵式都作为推理规则（见表 3-20），同时，一个基本等值式（见表 3-21）相当于两个基本逻辑蕴涵式. 除必须记住表 3-20 和表 3-21 之外，还要使用两个最基本的推理规则.

① **P 规则**. 所给的前提在证明过程中随时可以引用.

② **T 规则**. 已经推出的公式在以后的证明过程中可以随时引用.

表 3-21 基本等值式 E

(1) $\neg\neg A=A$（对合律）
(2) $A\vee A=A, A\wedge A=A$（幂等律）
(3) $A\vee B=B\vee A$ ，$A\wedge B=B\wedge A$（交换律）
(4) $(A\vee B)\vee C=A\vee(B\vee C)$，$(A\wedge B)\wedge C=A\wedge(B\wedge C)$（结合律）
(5) $A\vee(A\wedge B)=A, A\wedge(A\vee B)=A$（吸收律）
(6) $A\vee(B\wedge C)=(A\vee B)\wedge(A\vee C), A\wedge(B\vee C)=(A\wedge B)\vee(A\wedge C)$（分配律）
(7) $A\vee\neg A=1, A\wedge\neg A=0$（互补律：$A$ 有补元 $\overline{A}$）
(8) $\overline{A\vee B}=\overline{A}\wedge\overline{B}, \overline{A\wedge B}=\overline{A}\vee\overline{B}$（De Morgan 律）
(9) $A\vee 0=0\vee A=A$，$A\wedge 1=1\wedge A=A$（$\vee,\wedge$ 有单位元或称为同一律）
(10) $A\vee 1=1\vee A=1$，$A\wedge 0=0\wedge A=0$（$\vee,\wedge$ 有零元或称为 0-1 律）
(11) $A\rightarrow B=\neg A\vee B$
(12) $A\leftrightarrow B=(A\rightarrow B)\wedge(B\rightarrow A)$

自然推理系统的显著特点是没有公理，作为推理依据的只有推理规则. 这似乎更符合人们日常思维的推理习惯，因此称为自然推理.

在进行自然推理时，采用构造性证明方法，简称“**构造法**”，更准确地应该说是数理逻辑中的演绎(deduction)法，也可以称为“**形式证明**”. 在逻辑推理系统中，推出符号一般采用“$\vdash$”，但前面介绍的自然推理系统与公理化推理系统还是有很大区别的，所以按最接近于人的思维方式去理解，推出符号仍用“$\Rightarrow$”.

先通过一个例子了解证明的书写格式.

【例 3-30】 使用构造法证明：$p\rightarrow(q\vee r)$，$\neg s\rightarrow\neg q$，$p\wedge\neg s\Rightarrow r$.

证

(1) $p\wedge\neg s$	P
(2) p	T(1)I
(3) $\neg s$	T(1)I
(4) $p\rightarrow(q\vee r)$	P
(5) $q\vee r$	T(2)(4)I
(6) $\neg s\rightarrow\neg q$	P
(7) $\neg q$	T(3)(6)I
(8) r	T(5)(7)I

从证明过程可以看出，每一行由 3 部分组成：第一部分是编号，说明它是证明的第几步；第二部分仅写一个命题公式，实际上编号也说明了它是第几个命题公式；第三部分是写理由，交代该命题公式是怎样得来的.

初学者最感困难的是，如何一步一步地构造出从前提到结论的证明过程. 与其他证明题一样，可以先进行分析. 例 3-30 的分析过程如下：

要推出结论 r，在 3 个前提中，只有公式 $p\rightarrow(q\vee r)$ 中含有 r 且在后件 $q\vee r$ 中. 若能推出 p，则根据 $A\rightarrow B, A\Rightarrow B$ 即得 $q\vee r$，而这一点很容易办到，因为有前提 $p\wedge\neg s$. 在得到公式 $q\vee r$ 后，若能推出 $\neg q$，则利用 $A\vee B, \neg A\Rightarrow B$ 可得 r. 如何推出 $\neg q$? 在前提 $\neg s\rightarrow\neg q$ 含有 $\neg q$，只需要推出 $\neg s$ 即可，这一点也很容易办到，因为有前提 $p\wedge\neg s$.

【例 3-31】 使用构造法证明：$p\wedge\neg q\rightarrow r$，$\neg r\wedge\neg q\Rightarrow\neg p$.

证

(1) $p\wedge\neg q\rightarrow r$	P
(2) $\neg r\wedge\neg q$	P
(3) $\neg r$	T(2)I
(4) $\neg(p\wedge\neg q)$	T(1)(3)I
(5) $\neg p\vee q$	T(4)E
(6) $\neg q$	T(2)I
(7) $\neg p$	T(5)(6)I

一个推理形式是有效的，实际上是指符号推理是正确的. 要证明一个推理形式是有效的，首先将所给的前提和结论符号化，再根据定义 3-12 证明这个符号推理是正确的.

【例 3-32】 用构造法证明下列推理形式的有效性：如果小赵和小钱去上自习，则小孙也去. 小李不去自习或小赵去自习，由于小钱和小李已经去自习了，所以小孙也去上自习了.

解　用 p：小赵去自习，q：小钱去自习，r：小孙去自习，s：小李去自习，则要证明

$$(p \land q) \to r, \neg s \lor p, q \land s \Rightarrow r$$

(1) $q \land s$　　P

(2) q　　T(1)I

(3) s　　T(1)I

(4) $\neg s \lor p$　　P

(5) p　　T(3)(4)I

(6) $p \land q$　　T(2)(5)I

(7) $(p \land q) \to r$　　P

(8) r　　T(6)(7)I

下面介绍两种间接的构造性证明方法.

1. 反证法

要证明 $H_1, H_2, \cdots, H_n \Rightarrow C$，将结论 C 否定得到 $\neg C$，然后推出一个矛盾，如 $S \land \neg S$ 即可.

理由如下：要证明 $H_1, H_2, \cdots, H_n \Rightarrow C$，只要证 $H_1 \land H_2 \land \cdots \land H_n \to C$ 永真，即 $\neg(H_1 \land H_2 \land \cdots \land H_n) \lor C$ 永真，或者说证

$$\neg(\neg(H_1 \land H_2 \land \cdots \land H_n) \lor C) = H_1 \land H_2 \land \cdots \land H_n \land \neg C$$

永假，即得到一个永假式，如 $S \land \neg S$ 等.

【例 3-33】　使用反证法证明：$p \land \neg q \to r, \neg r \land \neg q \Rightarrow \neg p$.

证

(1) $\neg(\neg p)$　　P(附加)

(2) p　　T(1)E

(3) $\neg r \land \neg q$　　P

(4) $\neg q$　　T(3)I

(5) $p \land \neg q$　　T(2)(4)I

(6) $p \land \neg q \to r$　　P

(7) r　　T(5)(6)I

(8) $\neg r$　　T(3)I

(9) $r \land \neg r$　　T(7)(8)I

2. CP 规则(条件证明规则)

对于如下形式的推理：

$$H_1, H_2, \cdots, H_n \Rightarrow A \to C$$

只需要证明 $H_1, H_2, \cdots, H_n, A \Rightarrow C$，这就是采用 CP 规则的证明方法，它是将 $A \to C$ 的前件 A 和后件 C 分离的一种证明方法，称为**条件证明规则**.

理由如下：因为

$$\begin{aligned}
&(H_1 \land H_2 \land \cdots \land H_n) \to (A \to C) \\
&= \neg(H_1 \land H_2 \land \cdots \land H_n) \lor (\neg A \lor C) \\
&= (\neg(H_1 \land H_2 \land \cdots \land H_n) \lor \neg A) \lor C \\
&= \neg(H_1 \land H_2 \land \cdots \land H_n \land A) \lor C = (H_1 \land H_2 \land \cdots \land H_n \land A) \to C
\end{aligned}$$

所以，$(H_1 \land H_2 \land \cdots \land H_n) \to (A \to C)$ 永真的充要条件是 $(H_1 \land H_2 \land \cdots \land H_n \land A) \to C$ 永

真，即证明

$$H_1, H_2, \cdots, H_n, A \Rightarrow C$$

【例 3-34】 使用 CP 规则证明：$p \to (q \lor r), q \to \neg p, s \to \neg r \Rightarrow p \to \neg s$.

证

(1) $p \to (q \lor r)$	P
(2) p	P(附加)
(3) $q \lor r$	T(1)(2)I
(4) $q \to \neg p$	P
(5) $\neg q \lor \neg p$	T(4)E
(6) $\neg q$	T(2)(5)I
(7) r	T(3)(6)I
(8) $s \to \neg r$	P
(9) $\neg s \lor \neg r$	T(8)E
(10) $\neg s$	T(7)(9)I
(11) $p \to \neg s$	CP

数理逻辑的主要研究任务是建立一个严密的逻辑推理系统——公理推理系统来刻画人类的思维规律，这个系统与前面的自然推理系统是类似的，但它有更精简的初始符号、公式的形成规则、公理和推理规则. 已经有的逻辑演算形式系统，如 PC(formal system of Proposition Calculus)在理论上证明了其合理性、一致性、完备性等与语法和语义有关的重要结论，PC 能得出人类思维的所有推理规则，所提供的逻辑推理框架能保证在前提真的条件下，总能得出正确的结论. 对逻辑演算形式系统感兴趣，特别是做计算机软件工作的读者请参阅有关文献[14，15].

习 题 3.7

1. 对于命题公式 A, B，证明：$A \to B, \neg B \Rightarrow \neg A$.

2. 对于命题公式 A, B 和 C，证明：

(1) $A \land B \Rightarrow A$；

(2) $A \lor B, \neg A \Rightarrow B$；

(3) $A \to B, B \to C \Rightarrow A \to C$；

(4) $A \lor B, A \to C, B \to C \Rightarrow C$.

3. 证明下列推理形式是无效的：

(1) 若两个三角形全等，则其对应角相等；

(2) 两个三角形的对应角相等；

(3) 所以，这两个三角形全等.

4. 设 A, B 和 C 是命题公式，证明：

(1) $A \to B \Rightarrow (A \lor C) \to (B \lor C)$；

(2) $A \to B \Rightarrow (A \land C) \to (B \land C)$.

5. 设 A, B 是命题公式，则对于命题公式间的永真蕴涵关系 $\Rightarrow$ 有，$\inf\{A, B\} = A \land B$.

6. 使用构造法证明以下推理.

(1) $\neg(A \wedge B), B \vee C, \neg C \Rightarrow \neg A$.

(2) $A \to B, C \to A, C \Rightarrow B$.

7. 使用构造法证明以下推理.

(1) $A \wedge B, (A \leftrightarrow B) \to C \Rightarrow C$.

(2) $A \to B, (\neg B \vee C) \wedge \neg C, \neg(\neg A \wedge D) \Rightarrow \neg D$.

8. 使用反证法,构造出下面推理的证明.

(1) $\neg A \vee B, C \to \neg B, A \Rightarrow \neg C$.

(2) $A \to B, \neg(B \vee C) \Rightarrow \neg A$.

9. 使用 CP 规则,构造出下面推理的证明.

(1) $A \to (B \to C), \neg D \vee A, B \Rightarrow D \to C$.

(2) $A \to (B \to C), (C \wedge D) \to E, \neg F \to (D \wedge \neg E) \Rightarrow A \to (B \to F)$.

10. 证明下列公式是永真式.

(1) $(A \to B) \to ((A \to (B \to C)) \to (A \to C))$.

(2) $(A \to B) \to ((A \to \neg B) \to \neg A)$.

11. 证明下列推理形式的有效性：如果今天是星期四,则要进行离散数学或数据结构考试;如果数据结构老师有会,则不考数据结构;今天是星期四且数据结构老师有会,所以要进行离散数学考试.

12. 小东的爸爸带他出去玩,当乘车经过一座高楼时,爸爸对小东说："你只有现在好好学习,将来才能挣很多很多钱;有了很多很多钱,就能住上这样的高楼."小东听了爸爸的话,回答说："爸爸没有住上这样的高楼,是因为爸爸没有钱;爸爸没有钱是因为爸爸以前没有好好学习."请问：小东是否误解了爸爸原话的意思,为什么?

本章小结

1. 命题的有关概念

能判断出真假(或真假程度)的语句称为命题. 真命题真值为 1，假命题真值为 0. 不能分成更小的命题是原子命题，通常用小写英文字母 $p,q,r,s,\cdots$ 或带下标 p_1,p_2,p_3 等表示，否则是复合命题.

2. 逻辑联结词

1 元或 2 元逻辑运算共有 9 个，最基本的是 $\neg, \wedge, \vee$：

(1) $\neg p = \overline{p}$ 是 p 的否定，$\neg p$ 为 1 当且仅当 p 为 0.

(2) $p \wedge q = p \cdot q = pq$ 表示 p 并且 q，$p \wedge q$ 为 1 当且仅当 p 和 q 同时为 1.

(3) $p \vee q = p + q$ 表示 p 或 q，$p \vee q$ 为 0 当且仅当 p 和 q 同时为 0.

(4) $p \oplus q$ 表示 p 异或 q，p 和 q 不能同时为 1 的"或"，$p \oplus q$ 为 0 当且仅当 p 和 q 同时为 1 或同时为 0.

(5) $p \to q$ 表示"若 p，则 q"，$p \to q$ 为 0 当且仅当 p 为 1 且和 q 为 0.

(6) $p \leftrightarrow q$ 表示 p 当且仅当 q，$p \leftrightarrow q$ 为 1 当且仅当 p 和 q 取值相同.

(7) $p \uparrow q =: \neg(p \wedge q)$.

(8) $p \downarrow q =: \neg(p \vee q)$.

(9) $p \overset{n}{\rightarrow} q =: \neg(p \rightarrow q)$.

3. 命题公式及其真值表

命题公式就是逻辑函数或逻辑表达式，其中出现命题常量 0 和 1、命题变元和逻辑运算，但含义要清楚. 9 种运算 $\neg, \wedge, \vee, \oplus, \rightarrow, \leftrightarrow, \uparrow, \downarrow, \overset{n}{\rightarrow}$ 的级别按顺序从高到低.

将一个命题符号化后所得到的式子均为命题公式，于是对命题建立了数学模型—符号化，它也是抽象的一种方法. 命题符号化的步骤：第一步，找出所给命题的所有原子命题，并用小写英文字母或带下标表示；第二步，确定应使用的联结词，进而将原命题用符号表示出来.

命题公式的真值表就是该命题公式的取值情况表，要求能准确写出给定命题公式的真值表，当然记住逻辑运算表是至关重要的. 含 n 个命题变元的命题公式的真值指派有 2^n.

命题公式的分类：

$$\text{命题公式}\begin{cases}\text{可满足式}\begin{cases}\text{永真式}\\ \text{中性式}\end{cases}\\ \text{永假式}\end{cases}$$

4. 逻辑等值的命题公式

两个命题公式等值讨论的是它们之间的一种逻辑关系. 给定两个命题公式 A 和 B，$A=B$ 是指在任何真值指派下 A 和 B 的逻辑取值都相同.

基本等值式除与集合运算性质类似的那些外，特别要记住：

(1) $A \oplus B = \neg(A \leftrightarrow B)$.

(2) $A \rightarrow B = \neg A \vee B$.

(3) $A \leftrightarrow B = (A \rightarrow B) \wedge (B \rightarrow A)$.

由于等值关系是等价关系，可以按通常方式进行等值演算，特别在等值演算过程中可以使用“等值置换定理”.

理解命题公式的对偶式，了解对偶原理：设 A 和 B 是命题公式，若 $A=B$，则 $A^* = B^*$.

5. 命题公式的范式

由于等值关系是等价关系，需要考虑其等价类及其代表元. 命题公式的范式就是命题公式的标准形式或规范形式（作为代表元），要求能熟练得出给定命题公式的范式. 若 $A = A_1 \vee A_2 \vee \cdots \vee A_n (n \geqslant 1)$，其中 $A_i (1 \leqslant i \leqslant n)$ 是由命题变元或其否定组成的合取式，则称 $A_1 \vee A_2 \vee \cdots \vee A_n$ 为命题公式 A 的析取范式；若 $A = A_1 \wedge A_2 \wedge \cdots \wedge A_n (n \geqslant 1)$，其中 $A_i (1 \leqslant i \leqslant n)$ 是由命题变元或其否定组成的析取式，则称 $A_1 \wedge A_2 \wedge \cdots \wedge A_n$ 为命题公式 A 的合取范式.

根据命题公式中所有命题变元讨论其范式就得到命题公式的主范式：若 A 等值于由 A 中所有命题变元产生的若干个最小项的析取，则把后者称为 A 的主析取范式；若 A 等值于由 A 中所有命题变元产生的若干个最大项的合取，则把后者称为 A 的主合取范式.

要求掌握利用等值演算法和真值表法求出命题公式的范式，尤其是命题公式的主范式.

6. 联结词集合的功能完备性

由等值命题公式知道，1 元逻辑运算和 2 元逻辑运算的个数共 9 个. $\{\neg, \wedge, \vee\}$ 是功能

完备联结词集，进而$\{\downarrow\}$、$\{\uparrow\}$、$\{\neg,\wedge\}$、$\{\neg,\vee\}$和$\{\neg,\rightarrow\}$是功能完备的.

7. 命题逻辑的推理

设 $H_1,H_2,\cdots,H_n$ 和 C 是命题公式，若 $H_1,H_2,\cdots,H_n$ 全为真，可得出 C 必然真，则称由 $H_1,H_2,\cdots,H_n$ 得出 C 的推理形式是有效的，记为 $H_1,H_2,\cdots,H_n \Rightarrow C$. $H_1,H_2,\cdots,H_n \Rightarrow C$ 的充要条件是 $H_1 \wedge H_2 \wedge \cdots \wedge H_n \rightarrow C$ 是永真式，即 $H_1 \wedge H_2 \wedge \cdots \wedge H_n \Rightarrow C$.

记住最重要的基本逻辑蕴涵式：

$A \vee B, \neg A \Rightarrow B$（析取三段论）.

$A \rightarrow B, A \Rightarrow B$（假言推理）.

$A \rightarrow B, \neg B \Rightarrow \neg A$（拒取式）.

$A \rightarrow B, B \rightarrow C \Rightarrow A \rightarrow C$（假言三段论）.

$A \vee B, A \rightarrow C, B \rightarrow C \Rightarrow C$（二难推理）.

在进行推理时，采用的方法是构造法，是一种形式证明方法——只在符号之间进行. 需要通过一些训练才能熟练掌握. 同时，还要掌握两种间接的构造性证明方法：(1)反证法，(2)CP 规则（条件证明规则）.

第4章　谓词逻辑

原子命题是命题逻辑研究的基本单位，没有对原子命题的内部结构及其逻辑关系进行讨论.在实际思维中,仅有命题逻辑工具是不够的.例如著名的苏格拉底(Socrates)三段论.

大前提：所有的人都是要死的.

小前提：苏格拉底是人.

结论：所以,苏格拉底是要死的.

这个推理的有效性在命题逻辑中无法证明,因为上面的每个命题都是原子命题,可以分别用 p,q,r 表示,然而 $p,q\Rightarrow r$ 在命题逻辑中是无效推理.

之所以出现这种推理本身是正确的,但无法证明其有效性的问题,是因为没有对原子命题的内部形式结构及其逻辑关系进行讨论,这正是谓词逻辑首先要研究的内容,这些讨论涉及集合、映射、运算和关系.

本书讨论的谓词逻辑又称为一阶逻辑.

利用谓词逻辑建立起来的数据库设计理论,具有牢固的数学基础和一定的智能特点.同时,现实世界中的任何问题只要能用谓词逻辑推理系统方式表示出来,就可以将它写成逻辑程序设计(PROgramming in LOGic,PROLOG)或 LISP 语言,并用计算机加以实现,如机器人规划问题,已经开发出的一些智能教学专家系统等[15].

4.1　个体、谓词、量词和函词

4.1.1　个体

下面 4 个命题均为原子命题：

(1) 5 是素数；

(2) 3 大于 2；

(3) 张三是学生；

(4) 所有的人都是要死的.

上面出现的 5、3 和 2、张三以及人是命题分别考虑的对象,称为个体.命题的考虑对象称为**个体**(individual),它是独立存在的事物.个体可以是具体的,如 5、3 和 2、张三,也可以是抽象的,如人等.

表示特定的、具体的个体称为**个体常量**(constant),用 $a,b,c,\cdots,a_i,b_i,c_i,\cdots$ 等表示，如在(2)中,可以用 a：3,b：2，也可以直接用表示该个体常量的原符号表示,如“3”、“2”、“张三”等.不确定的个体称为**个体变元**(variable),用 $x,y,z,\cdots,x_i,y_i,z_i,\cdots$ 表示.

在讨论个体时,通常要指定个体讨论的范围,称为**个体域**(domain of individuals)或**论域**(universe),用 D 表示,一般假定 D 非空．如同时讨论(1)和(2)时,可以指定个体域为正整数集合,也可以是整数集合,还可以是实数集合等,要同时讨论(3)和(4),可以指定个体域

为所有人组成的集合,也可以是所有动物组成的集合等.指定个体域 D 后,所涉及的个体变元在所给的个体域中可任意取元素.

个体域可以是有限集合,可以是无限集合.我们把世界上所有对象,如所有的动物、所有植物、所有字母、所有数字等组成的集合称为**全总个体域**,简称**全域**,它是最大的个体域.之所以要给出这样的个体域,是因为在很多问题讨论时都没有指定个体域,这时就在全总个体域中讨论,它是默认的个体域.

4.1.2 谓词

(1) 中"…是素数",(3)中"…是学生",(4)中"…是要死的"是表示一个个体具有的性质,(2)中"…大于…"是表示两个个体之间的关系.我们把表示个体性质以及个体之间关系的词称为**谓词**(predicate).

表示一个个体性质的谓词称为 1 元谓词,表示 n 个个体之间关系的谓词称为 n 元谓词.一般用大写字母,如 $P,Q,R,\cdots$ 等表示谓词,对于任意的 n 元谓词,为了把谓词及其元数同时表示出来,像表示 n 元函数一样,用诸如 $P(x_1,x_2,\cdots,x_n)$表示.例如,用 $P(x)$:x 是素数,$S(x)$:x 是学生,$D(x)$:x 是要死的,$G(x,y)$:$x>y$,$R(x,y,z)$:x 通过 y 和 z 等.

需要说明的是,对于 n 元谓词中的元数 $n\geqslant 0$,若 $n=0$,n 元谓词表示命题常量 1、0 或命题变元.这样规定的目的是想把命题逻辑看作谓词逻辑的特例.

对于 n 元谓词 $P(x_1,x_2,\cdots,x_n)(n\geqslant 1)$,当个体变元 $x_1,x_2,\cdots,x_n$ 取定个体域中元素后就是一个命题,如 $G(x,y)$:$x>y$,它是关于命题的函数,称为**命题函数**(propositional function).显然,命题函数不是命题.

命题函数,如 $P(x_1,x_2,\cdots,x_n)$也可以表示为 $P^{(n)}x_1x_2\cdots x_n$.

注意 谓词的选取与个体域有关.例如,对于命题"所有人都是要死的",若在所有人组成的个体域 D 中考虑,只需一个谓词 $D(x)$:x 是要死的;若在全域中考虑,需要两个谓词 $P(x)$:x 是人,$D(x)$:x 是要死的,其中 $P(x)$称为**特性谓词**,使用这个特性谓词是将"人"从全域中分离出来.

4.1.3 量词

1. 量词的概念

对于命题函数,如 $P(x)$:x 是素数,在个体域 D 为自然数集合 $\mathbf{N}$ 时,对于 x 的每一个取值,就得到一个命题.使 $P(x)$成为命题的另一种方法是,量化个体变元 x.常使用的方法有两种:全称量化和存在量化.如 D 中任意 x 有 $P(x)$,即"任意自然数是素数",D 中存在 x 有 $P(x)$,即"有些自然数是素数",它们都是命题了.

把表示个体数量特征的词称为**量词**(quantifier),常用的量词有:**全称量词** $\forall$ (universal quantifier)和**存在量词** $\exists$ (existential quantifier).全称量词 $\forall$ 相当于"任意"、"全部"、"所有"、"每一个"、"一切"等,存在量词 $\exists$ 相当于"有些"、"某些"、"有的"、"存在"、"至少有一个"等.本书不涉及存在唯一量词 $\exists !$.

现在的量化仅对个体进行,不对谓词进行,因而称为一阶谓词逻辑.

2. 量词的使用

首先注意,量词单独使用是没有意义的,量词的后面一定要跟个体变元,如 $\forall x$, $\forall y$,…,

$\exists x$，$\exists y$，…，所以我们总是不区分 $\forall$ 与 $\forall x$，$\exists$ 与 $\exists x$，$\forall x$ 或 $\exists x$ 是一个整体. 量词后面所跟的个体变元称为**指导变元**. 例如，

$\forall xP(x)$：任意元素 x 都具有性质 P；

$\exists xP(x)$：存在元素 x 具有性质 P；

$\forall x\,\forall yG(x,y)$：对于任意元素 x 和 y 都具有关系 G；

$\forall x\,\exists yG(x,y)$：对于任意元素 x，存在元素 y，x 和 y 有关系 G；

$\exists x\,\forall yG(x,y)$：存在元素 x，对于任意元素 y，x 和 y 有关系 G；

$\exists x\,\exists yG(x,y)$：存在元素 x 和 y 有关系 G.

若将命题函数中的所有个体变元都进行了量化，则得到一个命题，否则不是命题. 如 $\forall xG(x,y)$ 表示对于任意元素 x 和元素 y，x 和 y 有关系 G，由于元素 y 可以是任意指定的个体，$\forall xG(x,y)$ 是一个与 y 有关的命题函数.

3. 量词与个体域

量词是对个体变元进行量化，所给的个体域 D 至关重要. 同一个带量词的命题，如 $\forall x\,\exists yG(x,y)$，而 $G(x,y)$：$x>y$，则在自然数集合 $\mathbf{N}$ 中，$\forall x\,\exists yG(x,y)$ 表示没有最小的自然数，是假命题，而在整数集合 $\mathbf{Z}$ 中，$\forall x\,\exists yG(x,y)$ 表示没有最小的整数，是真命题.

可以按个体域 $D=\mathbf{N}$，$P(x)$：x 是素数，$G(x,y)$：$x>y$，去理解上小节关于量词的使用，特别是多重量词的使用.

前面已经说明，全域 D 是默认个体域. 对于给定的个体域 D，请注意区分下列表达式的不同含义：

(1) $\forall xP(x)$ 表示任意 D 中元素 x 具有性质 P. $\forall xP(x)$ 是命题，当 D 中任意元素 x 都具有性质 P 时是真命题，否则是假命题.

(2) $P(x)$ 表示 D 中元素 x 具有性质 P. $P(x)$ 是命题函数.

(3) $\exists xP(x)$ 断定至少存在 D 中一个个体 x 具有性质 P，至于是哪一个个体没有给出. $\exists xP(x)$ 是命题，若 D 中至少有一个个体具有性质 P 时是真命题，否则是假命题.

(4) $P(a)$ 表示 D 中个体常量 a 具有性质 P. $P(a)$ 断定元素 a 具有性质 P，$P(a)$ 是命题，其真假值由元素 a 决定. 显然，$P(a)$ 真则 $\exists xP(x)$ 真，但 $\exists xP(x)$ 真不能得出 $P(a)$ 真.

4. 量词的辖域、约束变元与自由变元

若令 $P(x)$：x 是人，$D(x)$：x 是要死的，则“所有的人都是要死的”可以表示为 $\forall x(P(x)\rightarrow D(x))$，这时 $\forall x$ 的作用或管辖范围为 $P(x)\rightarrow D(x)$，其中两次出现的 x 是约束变元.

若令 $Q(x)$：x 是有理数，$R(x)$：x 是实数，则“有些实数是有理数”可以表示为 $\exists x(R(x)\wedge Q(x))$，这时 $\exists x$ 的作用或管辖范围为 $R(x)\wedge Q(x)$，其中两次出现的 x 是约束变元.

量词 $\forall x$ 或 $\exists x$ 的作用或管辖的范围称为 $\forall x$ 或 $\exists x$ 的**作用域**或**辖域**(scope)，辖域内的个体变元 x 称为**约束变元**(bound variable). 若量词后有括号，则括号里面的部分是其辖域. 例如在 $\forall x(P(x)\rightarrow D(x))$ 中 $P(x)\rightarrow D(x)$ 是 $\forall x$ 的辖域，两次出现的 x 是约束变元；若没有括号，则与量词相邻的部分是辖域. 如 $\exists xP(x)$ 中 $\exists x$ 的辖域是 $P(x)$，$P(x)$ 中的 x 是约束变元. 特别注意，在 $\forall x\,\exists yG(x,y)$ 中，$\exists y$ 的辖域是 $G(x,y)$，而 $\forall x$ 的辖域是 $\exists yG(x,y)$.

不受任何量词约束的变元称为**自由变元**(free variable). 例如 $\forall xG(x,y)$ 中的 y，它不受

$\forall x$ 的约束，这时 $G(x,y)$中的 y 是自由变元.

请自己分析 $\exists x(R(x)\wedge Q(x))$与 $\exists xR(x)\wedge Q(x)$的不同之处.

5. 约束变元与自由变元的改名(rename)

对于第 4.1.2 小节中的“所有人都是要死的”，也可以 $\forall y(P(y)\rightarrow D(y))$，或 $\forall z(P(z)\rightarrow D(z))$，这说明可以对约束变元改名. 同样可以对自由变元改名，如 $\forall xG(x,y)$中 $G(x,y)$里出现的 y 可以改成 z,w,t 等，就是不能改成 x，否则自由变元改成了约束变元，又如 $\exists xR(x)\wedge Q(x)$中在 $Q(x)$里面出现的 x 可以改成 y,z 等.

这与定积分与积分变量无关是类似的：$\int_a^b f(x)\mathrm{d}x=\int_a^b f(y)\mathrm{d}y$.

之所以要改名，一是为了避免同一个个体变元既是约束的又是自由的；二是为了方便后面计算谓词公式的范式.

注意 在对个体变元改名时，①将量词辖域中某约束变元及相应的指导变元改成本辖域中未曾出现过的(约束或自由)个体变元，其他个体变元不变；②某自由变元全部改成同一个与出现的其他所有个体变元不同的个体变元.

4.1.4 函词

要把如“张三的父亲”、“两个数的平方和”等表示出来，就要用函数，在谓词逻辑中习惯称为**函词**(function).

设个体域 D 为所有人组成的集合，$f(x)$：x 的父亲，则 f 是 D 上(即 D 到 D)的 1 元函数. 令 $D=\mathbf{R}$，$f(x,y)=x^2+y^2$，则 f 是 D 上(即 D^2 到 D)的 2 元函数.

习 题 4.1

1. 对于命题“3 是素数”，列举出 3 个个体域.

2. 分别在整数集合 $\mathbf{Z}$ 和实数集合 $\mathbf{R}$ 中，确定命题“所有整数是有理数”中的谓词.

3. 找出下列原子命题中的个体常量、谓词、量词及函词，并用符号分别表示出来.

(1) 小赵是工人.

(2) 张三的父亲是李四.

(3) -3 是有理数.

(4) 米卢喜欢踢足球.

(5) 所有有理数是实数.

(6) 有些实数是有理数.

(7) 北京举办 2008 年奥运会.

(8) 每个人都要锻炼身体.

4. 用 $E(x,y)$：x 选修 y，其中 x 所在个体域为班上全体同学组成的集合，y 所在个体域为所有开设的计算机课程组成的集合，用命题分别表示：

(1) $\forall x\exists yE(x,y)$； (2) $\forall x\forall yE(x,y)$；

(3) $\exists x\exists yE(x,y)$； (4) $\exists x\forall yE(x,y)$；

(5) $\forall y\exists xE(x,y)$； (6) $\forall y\forall xE(x,y)$；

(7) $\exists y \exists x E(x,y)$;　　　　(8) $\exists y \forall x E(x,y)$.

5. 分别指出下列各式中各量词的辖域及个体变元的约束情况.

(1) $\forall x(P(x) \vee \exists y R(y)) \rightarrow Q(x)$.

(2) $\forall x \exists y(P(x,y) \wedge Q(y,z)) \wedge \exists x P(x,y)$.

(3) $\forall x(P(x) \wedge \exists x Q(x)) \vee (\forall x P(x) \rightarrow Q(x))$.

(4) $\forall x \forall y(R(x,y) \vee L(z,y)) \wedge \exists x S(x,y)$.

6. 对 $\exists x P(x) \wedge \exists x Q(x)$ 中 $\exists x Q(x)$ 的约束变元 x 改名.

7. 对 $\forall x(P(x,y) \wedge \exists y Q(x,y))$ 中的自由变元 y 改名.

4.2　谓词公式及命题的符号化

4.2.1　谓词公式

谓词公式(predicate formula)简称公式,同命题公式一样采用的是递归定义.通过例子给出谓词公式的定义.

1. 对应任意自然数 n,n 元谓词 P 和 n 个任意个体 $t_1,t_2,\cdots,t_n$,$P(t_1,t_2,\cdots,t_n)$ 是谓词公式

n 个任意个体 $t_1,t_2,\cdots,t_n$ 是指 $t_i(1 \leqslant i \leqslant n)$ 可以是个体常量、个体变元,也可以是用函词表示的个体常量或个体变元,这些 $t_i(1 \leqslant i \leqslant n)$ 称为**项**(term).

若 $n=0$,$P(t_1,t_2,\cdots,t_n)$ 表示个体常量 1、0 或命题变元.

用 p: $3>2$;$O(x)$: x 是年老的;$G(x,y)$: $x>y$;$I(f(x),y)$: x 的父亲是 y;$E(a,y)$: $a=y$ 等,这时 p,$O(x)$,$G(x,y)$,$I(f(x),y)$,$E(a,y)$ 都是谓词公式.

2. 若 A 是谓词公式,则 $\neg A$ 是谓词公式

用 a: 小赵,$W(x)$: x 是工人,则"小赵不是工人"表示为 $\neg W(a)$,$\neg W(a)$ 是谓词公式.

用 $P(x)$: x 是素数,则 $\neg P(x)$ 是谓词公式.

3. 若 A 和 B 是谓词公式,则 $A * B$ 是谓词公式,其中 $*$ 是 2 元逻辑联结词

以 $Q(x)$: x 是有理数,$R(x)$: x 是实数,则 $R(x) \wedge Q(x)$,$Q(x) \rightarrow R(x)$ 等是谓词公式.

以 $B(x)$: x 是男生,$G(x)$: x 是女生,则 $B(x) \oplus G(x)$ 是谓词公式.

4. 若 A 是谓词公式,则 $\forall x A$, $\exists x A$ 是谓词公式

例如,$Q(x)$: x 是有理数,$R(x)$: x 是实数,则 $\exists x(R(x) \wedge Q(x))$, $\forall x(Q(x) \rightarrow R(x))$ 等是谓词公式.

若 $G(x,y)$: $x>y$,则 $\exists y G(x,y)$ 及 $\forall x \exists y G(x,y)$ 等是谓词公式.

5. 有限次使用上面的 1.～4. 得到的符号串是仅有的谓词公式

显然,$\neg \forall x(R(x) \rightarrow Q(x))$, $\forall x \forall y(P(x,y) \wedge Q(y,z)) \wedge \exists x P(y,x)$ 等是谓词公式.

跟命题公式的理解一样,只要是书写正确、意义清楚的符号串或表达式是谓词公式.由于在(1)中规定了命题常量和命题变元是谓词公式,所以命题公式是谓词公式.

通常,将不含自由变元的谓词公式称为**闭**(**closed**)公式,否则称为**开**(**open**)公式.

4.2.2　命题的符号化

与命题逻辑中命题的符号化不同,我们是在谓词逻辑或一阶逻辑中将命题符号化,它要

求必须使用谓词.

在谓词逻辑中将命题符号化，首先找出所给命题中的所有个体常量，并用 $a,b,c,\cdots,a_i,b_i,c_i,\cdots$ 表示；其次是确定在给定个体域中应该选用的所有谓词，特别注意特性谓词的选取；再其次是确定量词；再次确定函词；最后通过找出联结词，将所给命题符号化.

在谓词逻辑中将命题符号化是本章重点内容之一，这种形式化方法和技巧在软件测试、软件工程及软件理论等研究中是至关重要的.

再看下面的例子.

【例 4-1】 在谓词逻辑中，将下列命题符号化.

(1) 小孙选修模糊数学或人工智能课程.

(2) 米卢教练是年老的但是健壮的.

解 (1) 用 a：小孙，$F(x)$：x 选修模糊数学，$A(x)$：x 选修人工智能，则原命题符号化为 $F(a)\vee A(a)$.

(2) 用 b：米卢，$O(x)$：x 是年老的，$S(x)$：x 是健壮的，则原命题符号化为 $O(b)\wedge S(b)$.

【例 4-2】 在谓词逻辑中，将下列命题符号化.

(1) 所有有理数是实数.

(2) 有些实数是有理数.

解 令 $R(x)$：x 是实数，$Q(x)$：x 是有理数，则

(1) $\forall x(Q(x)\rightarrow R(x))$.

(2) $\exists x(R(x)\wedge Q(x))$.

注意 在命题符号化而不是一般地讨论谓词公式时，(1) 不能符号化为 $\forall x(Q(x)\wedge R(x))$；(2) 不能符号化为 $\exists x(R(x)\rightarrow Q(x))$，只要把谓词公式 $\forall x(Q(x)\wedge R(x))$ 和 $\exists x(R(x)\rightarrow Q(x))$ 表示的意义用文字表达出来就明显了.

【例 4-3】 在谓词逻辑中，将下列命题符号化.

(1) 每个人都有自己的爱好.

(2) 有的整数不是自然数.

解 (1) 用 $P(x)$：x 是人，$H(x)$：x 有自己的爱好，则原命题符号化为

$$\forall x(P(x)\rightarrow H(x))$$

(2) 用 $N(x)$：x 是自然数，$Z(x)$：x 是整数，则原命题符号化为

$$\exists x(Z(x)\wedge \neg N(x))$$

【例 4-4】 在谓词逻辑中，将下列命题符号化.

(1) 没有一个自然数大于等于任意自然数.

(2) 存在唯一的偶素数.

解 (1) 用 $N(x)$：x 是自然数，$G(x,y)$：$x\geqslant y$，则原命题符号化为

$$\neg\exists x(N(x)\wedge\forall y(N(y)\rightarrow G(x,y)))$$

(2) 用 $E(x)$：x 是偶数，$P(x)$：x 是素数，$I(x,y)$：$x=y$，则原命题符号化为

$$\exists x(E(x)\wedge P(x)\wedge\forall y(E(y)\wedge P(y)\rightarrow I(x,y)))$$

【例 4-5】 在谓词逻辑中，将命题“经过两个不同的点有且仅有一条直线”符号化.

解 用 $P(x)$：x 是点，$L(x)$：x 是线，$E(x,y)$：$x=y$，$R(x,y,z)$：z 通过 x 和 y，则原命

题符号化为

$$\forall x \forall y(P(x) \land P(y) \land \neg E(x,y) \to \exists z(L(z) \land R(x,y,z) \land \forall w(L(w) \land R(x,y,w) \to E(z,w))))$$

【例 4-6】 在谓词逻辑中，将下列命题符号化.

(1) 没有最大的素数.

(2) 并非所有的素数都不是偶数.

(3) 任意大于 4 的偶数都是两个奇素数之和(这是著名的哥德巴赫猜想：1+1 = 2).

解 用 $P(x)$：x 是素数，$E(x)$：x 是偶数，$O(x)$：x 是奇数，$G(x,y)$：$x>y$，$F(x)$：$x>4$，$f(x,y)=x+y$，$I(x,y)$：$x=y$，则：

(1) $\neg \exists x(P(x) \land \forall y(P(y) \land \neg I(x,y) \to G(x,y)))$.

(2) $\neg \forall x(P(x) \to \neg E(x))$.

(3) $\forall x(F(x) \land E(x) \to \exists y \exists z(O(y) \land O(z) \land P(y) \land P(z) \land I(x,f(y,z))))$.

【例 4-7】 在谓词逻辑中，将下列命题符号化.

(1) 只有总经理才有秘书.

(2) 任何驯服的马都受过良好训练.

解 (1) 用 $M(x)$：x 是总经理，$S(x)$：x 有秘书，则原命题符号化为

$$\forall x(S(x) \to M(x))$$

(2) 用 $H(x)$：x 是马，$T(x)$：x 是驯服的，$W(x)$：x 受过良好训练，则原命题符号化为

$$\forall x(H(x) \land T(x) \to W(x))$$

注意 命题的符号化是没有止境的.例如在例 4-7(1)中，还可以对“总经理”、“秘书”等进一步符号化.只做到能表明命题的意思，满足后面对推理有效性讨论要求就可以了.

习 题 4.2

1. 在谓词逻辑中符号化下列命题.

(1) 小李不是学生，是老师.

(2) 人人都会犯错误.

(3) 有些大学生是体育爱好者.

(4) 凡是老虎都是要吃人的.

(5) 不可能每位研究生都是科研人才.

(6) 任意整数不是偶数就是奇数.

(7) 每一个大学生都钦佩某位老师.

(8) 有些大学生不喜欢《超级女声》.

(9) 姚明是 NBA 球员，杨利伟去过太空.

(10) 不管黑猫白猫，抓住老鼠就是好猫.

2. 在谓词逻辑中符号化下列命题.

(1) 每个人都是专家且是教师.

(2) 有些人是青年人.

(3) 有些人是青年专家.

3. 在谓词逻辑中符号化下列命题.

(1) 自然数都是整数.

(2) 整数都是有理数.

(3) 有的整数不是自然数.

(4) 有的有理数不是整数.

(5) 自然数都是有理数并且存在既不是自然数又不是整数的有理数.

4. 假定个体域为所有人组成的集合,在谓词逻辑中符号化下列命题.

(1) 每个喜欢步行的人都不喜欢坐车.

(2) 每个人或者喜欢骑自行车或者喜欢坐车.

(3) 并非每个人都喜欢骑自行车.

(4) 有些人不喜欢步行.

5. 在谓词逻辑中符号化下列命题.

(1) 所有牛都有角.

(2) 有些动物是牛.

(3) 有些动物有角.

6. 在谓词逻辑中符号化下列命题.

(1) 鸟会飞.

(2) 猴子不会飞.

(3) 猴子不是鸟.

7. 假定个体域为所有人组成的集合,在谓词逻辑中符号化下列命题.

(1) 每个学生或是勤奋的或是聪明的.

(2) 所有勤奋的人都会有所作为.

(3) 并非每个学生都有所作为.

(4) 有些学生是聪明的.

8. 在谓词逻辑中符号化下列命题.

(1) 桌上的每本书都是杰作.

(2) 写出杰作的人都是天才.

(3) 某个不出名的人写了桌上的某本书.

(4) 某个不出名的人是天才.

9. 在谓词逻辑中符号化下列命题.

(1) 兔子比乌龟跑得快.

(2) 有的兔子比所有乌龟跑得快.

(3) 并不是所有兔子都比乌龟跑得快.

(4) 没有跑得同样快的两只兔子.

10. 使用谓词将“金子是闪光的,但闪光的未必是金子”符号化.

4.3 谓词公式的解释及类型

4.3.1 谓词公式的解释

谓词公式的取值(1 或 0),取决于对其进行的解释或赋值,它类似于对命题公式的指派,其重要性是显而易见的. 但与命题公式不同的是,谓词公式的解释有无限多种,每种**解释**(interpretation)I 由下面 5 部分组成,结合谓词公式 $\forall x(P(z)\wedge\exists yQ(f(x,y),a))\wedge r$ 进行说明.

(1) 指定个体域 D.

个体域 D 可以是有限集合,也可以是无限集合. 为了方便,取 $D=\{1,2\}$.

(2) 对于谓词公式中的命题变元指派其真值.

在谓词公式 $\forall x(P(z)\wedge\exists yQ(f(x,y),a))\wedge r$ 中,r 是命题变元,可取 $r=1$.

(3) 对于谓词公式中的个体常量及其自由变元解释为指定个体域 D 中的元素.

谓词公式中的个体常量为 a, 应解释为 D 中某个体, 如$\frac{a}{2}$,它表示 a 取 D 中元素 2;对于公式中的自由变元 z,它可以在 D 中任意取值,但对它进行解释时,还得要任意指定 D 中一个元素,如$\frac{z}{2}$.

(4) 对于谓词公式中的函词解释为 D 上的函数.

在谓词公式 $\forall x(P(z)\wedge\exists yQ(f(x,y),a))\wedge r$ 中,f 是一个 2 元函词,可以将 f 解释为如下的 D 上的 2 元函数:

$$f(1,1)=2,\quad f(1,2)=1,\quad f(2,1)=1,\quad f(2,2)=2,$$

也可以写成$\frac{f(1,1)}{2},\frac{f(1,2)}{1},\frac{f(2,1)}{1},\frac{f(2,2)}{2}$这种形式.

(5) 对于谓词公式中的谓词解释为 D 上的谓词.

在谓词公式 $\forall x(P(z)\wedge\exists yQ(f(x,y),a))\wedge r$ 中,P 是 1 元谓词,Q 是 2 元谓词,对谓词进行解释,有两种方式:

① 根据谓词定义,可以将 P 解释为 $P(x)$: x 是素数,将 Q 解释为 $Q(x,y)$: $x>y$.

② 根据命题函数的定义,$\frac{P(1)}{0},\frac{P(2)}{1};\frac{Q(1,1)}{0},\frac{Q(1,2)}{0},\frac{Q(2,1)}{1},\frac{Q(2,2)}{0}$.

上述两种对谓词的解释方式①,②是相同的.

谓词公式在任何解释 I 下都会取得一个真值. 在求其真值之前,再回忆一下,4.1 节在给定个体域 D 后关于 $\forall xP(x)$ 和 $\exists xP(x)$ 的理解. 实际上,若 D 为有限集合: $D=\{d_1,d_2,\cdots,d_m\}$,请记住下面两个**消去量词的逻辑等值式**:

$$\forall xP(x)=P(d_1)\wedge P(d_2)\wedge\cdots\wedge P(d_m)$$

$$\exists xP(x)=P(d_1)\vee P(d_2)\vee\cdots\vee P(d_m)$$

因此,

$$\forall x(P(z)\wedge\exists yQ(f(x,y),a))\wedge r=\forall x(P(2)\wedge\exists yQ(f(x,y),2))\wedge 1$$
$$=\forall x(P(2)\wedge\exists yQ(f(x,y),2))=\forall x\exists yQ(f(x,y),2)$$

$=\forall x(Q(f(x,1),2) \vee Q(f(x,2),2))$

$=(Q(f(1,1),2) \vee Q(f(1,2),2)) \wedge (Q(f(2,1),2) \vee Q(f(2,2),2))$

$=(Q(2,2) \vee Q(1,2)) \wedge (Q(1,2) \vee Q(2,2))$

$=(0 \vee 0) \wedge (0 \vee 0) = 0$

再看一个例子.

【例 4-8】 求下列两个谓词公式.

(1) $\forall x(A(x) \vee B(x))$;

(2) $\forall xA(x) \vee \forall xB(x)$.

在给定解释 I：$D=\mathbf{Z}$,$A(x)$：x 是偶数,$B(x)$：x 是奇数下的真值.

解 (1) 在所给解释 I 下,$\forall x(A(x) \vee B(x))$表示“任意整数是偶数或奇数”是真命题.

(2) 在所给解释 I 下,$\forall xA(x)$表示“任意整数是偶数”是假命题,$\forall xB(x)$表示“任意整数是奇数”是假命题,于是 $\forall xA(x) \vee \forall xB(x)$在所给解释 I 下取假.

4.3.2 谓词公式的类型

【定义 4-1】 在任何解释下均为真的谓词公式称为**永真式**或**有效式**(valid).

下面的例子说明,在谓词逻辑中是如何证明一个公式是永真式的.

【例 4-9】 证明谓词公式 $\forall xA(x) \rightarrow A(t)$永真.

证 任意给定个体域 D 上的解释 I,假定 $\forall xA(x)$在该解释下取 1,则对于任意 $d \in D$,$A(d)$取 1, 于是 $A(t)$为 1.

【例 4-10】 证明谓词公式 $\forall xA(x) \vee \forall xB(x) \rightarrow \forall x(A(x) \vee B(x))$永真.

证 任意给定个体域 D 上的解释 I,假定 $\forall xA(x) \vee \forall xB(x)$在该解释下取 1,则 $\forall xA(x)$或$\forall xB(x)$取 1, 这时 $\forall x(A(x) \vee B(x))$取 1, 因此 $\forall xA(x) \vee \forall xB(x) \rightarrow \forall x(A(x) \vee B(x))$永真.

【例 4-11】 证明谓词公式 $\exists x \forall yA(x,y) \rightarrow \forall y \exists xA(x,y)$永真.

证 任意给定个体域 D 上的解释 I,假定 $\exists x \forall yA(x,y)$在该解释下取 1,则存在 $d_0 \in D$,对于任意 $d \in D$,有 $A(d_0,d)$为 1,所以 $\forall y \exists xA(x,y)$为 1.

对于命题逻辑中的任何永真式,如$(p \rightarrow q) \wedge p \rightarrow q$,分别用任意谓词公式 A,B 去全部替换命题变元 p,q 所得到的谓词公式,$(A \rightarrow B) \wedge A \rightarrow B$ 是永真式. 这一点是显然的.

【定义 4-2】 至少存在一种解释使其为 1 的谓词公式称为**可满足式**(satisfactable formula),否则称为不可满足式或矛盾式或**永假式**(contradiction). 既存在取 1 的解释,又存在取 0 的解释的谓词公式称为**中性式**或**偶然式**(contingency).

1936 年丘奇(Church)和图灵(Turing)分别独立证明了：中性谓词公式无法在有限步内判定;永真(或永假)谓词公式可在有限步内判定.

习 题 4.3

1. 设个体域 $D=\{a,b,c\}$,消去下列谓词公式中的量词.

(1) $\forall xP(x) \wedge \exists xQ(x)$.

(2) $\forall x(P(x) \rightarrow \exists yQ(y))$.

(3) $\forall x \exists y R(x,y)$.

(4) $\exists y \forall x R(x,y)$.

2. 对于以下谓词公式的解释.

个体域 $D=\{1,2\}$.

个体常量：$\dfrac{a}{1},\dfrac{b}{2}$.

函词 f：$\dfrac{f(1)}{2},\dfrac{f(2)}{1}$.

谓词 P：$\dfrac{P(1,1)}{1},\dfrac{P(1,2)}{1},\dfrac{P(2,1)}{0},\dfrac{P(2,2)}{0}$.

分别求下列谓词公式在上述解释下的真值.

(1) $P(f(a),a) \wedge P(f(b),b)$.

(2) $\exists y \forall x P(y,x)$.

(3) $\forall x \exists y (P(f(x),f(y)) \rightarrow P(x,y))$.

3. 求下列两个谓词公式. 在给定解释 I：$D=\mathbf{Z}$, $A(x)$：x 是偶数, $B(x)$：x 是奇数下的真值.

(1) $\exists x (A(x) \wedge B(x))$.

(2) $\exists x A(x) \wedge \exists x B(x)$.

4. 设个体域 $D=\mathbf{Z}$, 定义如下谓词 $N(x)$：x 是正整数, $P(x)$：x 是素数, $E(x,y)$：$x=y$, $L(x,y)$：$x<y$, $D(x,y)$：$x \mid y$, 判断下列谓词公式在上述解释下的真值.

(1) $\forall x (P(x) \rightarrow \exists y (P(x) \wedge L(x,y) \wedge D(x,y)))$.

(2) $\forall x (P(x) \leftrightarrow \forall y (P(y) \wedge L(y,x) \rightarrow \neg D(y,x)))$.

(3) $\forall x (N(x) \rightarrow \exists y \exists z (P(y) \wedge P(z) \wedge \neg E(y,z) \wedge D(y,z) \wedge D(z,x)))$.

(4) $\exists x (P(x) \wedge \forall y (P(y) \wedge \neg E(x,y)) \rightarrow L(y,x))$.

5. 分别找出使下列谓词公式取 1 的解释.

(1) $\forall x \exists y (P(f(x,y),a) \rightarrow P(x,y))$.

(2) $\exists x Q(g(x)) \wedge \forall y P(x,y)$.

6. 分别找出使下列谓词公式取 0 的解释.

(1) $\forall x A(x,x) \rightarrow \exists y \forall x A(x,y)$.

(2) $(\exists x P(x) \rightarrow \exists y Q(y)) \wedge \exists y Q(y) \rightarrow \exists x P(x)$.

7. 证明谓词公式 $\exists x (A(x) \vee B(x)) \rightarrow \exists x A(x) \vee \exists x B(x)$ 永真.

8. 证明下列谓词公式永真.

(1) $\forall x A(x) \rightarrow \exists x A(x)$.

(2) $\forall x \forall y A(x,y) \rightarrow \forall x \exists y A(x,y)$.

(3) $\forall x \exists y A(x,y) \rightarrow \exists x \exists y A(x,y)$.

9. 设个体域 $D=\{a,b\}$, 构造使 $\forall x (A(x) \rightarrow B(x)) \leftrightarrow (\exists x A(x) \rightarrow \forall x B(x))$ 为 0 的解释.

10. 给出使以下谓词公式为 1 和为 0 的解释.

(1) $\exists x A(x) \rightarrow \forall x A(x)$.

(2) $\forall x \neg A(x,x) \wedge \forall x \exists y A(x,y) \wedge \forall x \forall y \forall z (A(x,y) \wedge A(y,z) \rightarrow A(x,z))$.

11. 给出使以下谓词公式为 1 和为 0 的解释.

(1) $\exists xA(x)\to A(b)$.

(2) $\forall x\forall y(A(x,y)\to A(y,x))$.

12. 给出使以下谓词公式为 1 和为 0 的解释.

(1) $\forall x(A(x)\to\exists y(B(y)\land C(x,y)))$.

(2) $\forall x\forall y(A(x,y)\to\neg A(y,x))$.

4.4 逻辑等值的谓词公式

4.4.1 谓词公式等值的定义

与两个命题公式等值完全类似,有

【定义 4-3】 设 A,B 是谓词公式,若 A 和 B 在任何解释下的取值都相同,则称 A 和 B 是**逻辑**等值的,记为 $A=B$.

显然,$A=B$ 的充要条件是谓词公式 $A\leftrightarrow B$ 永真.

根据命题逻辑中的等值式容易得到一些谓词逻辑中的等值式.例如,对于命题变元 p,q,有 $p\to q=\neg p\lor q$,因为$(p\to q)\leftrightarrow(\neg p\lor q)$永真,所以对于谓词公式 A 和 B,有$(A\to B)\leftrightarrow(\neg A\lor B)$,进而有 $A\to B=\neg A\lor B$.照这种方式,可以得到很多谓词逻辑中的等值式,参见 3.4 节定理 3-5 和定理 3-6 或 3.7 节表 3-24.

4.4.2 基本等值式

下面 10 个与量词有关的等值式是谓词逻辑中的基本等值式.

1. 量词转换

(1) $\neg\forall xA(x)=\exists x\neg A(x)$.

(2) $\neg\exists xA(x)=\forall x\neg A(x)$.

这是两个 $\forall x$ 与 $\exists x$ 相互转换的等值式.

【例 4-12】 举例说明上述等值式(1)、(2)成立.

解 令 D 是全班所有同学组成的集合,$A(x)$:x 今天来上课,则"并非每位同学今天都来上课"等价于"有同学今天没有来上课","并非有同学今天来上课"等价于"每位同学今天都没有来上课".

2. 量词辖域的收缩与扩张

设 B 中不含自由变元 x,则有

(1) $\forall x(A(x)\land B)=\forall xA(x)\land B$.

(2) $\forall x(A(x)\lor B)=\forall xA(x)\lor B$.

(3) $\exists x(A(x)\land B)=\exists xA(x)\land B$.

(4) $\exists x(A(x)\lor B)=\exists xA(x)\lor B$.

首先要说明的是,$A(x)$含自由变元 x,而 B 中不含自由变元 x,但 $A(x)$和 B 都可能含其他自由变元.

就(1)来说,左边 $\forall x$ 的辖域为 $A(x)\land B$,右边 $\forall x$ 的辖域为 $A(x)$,从左边到右边量词的

辖域收缩了，而从右边到左边量词的辖域扩张了.

可以粗略地这样理解，因为 B 中不含自由变元 x，所以 $\forall x$ 及 $\exists x$ 对 B 都不起作用.

(1)的证明：对于任意的个体域 D 上的解释 I，假定 $\forall x(A(x)\wedge B)$真，则对于任意 $d\in D$，$A(d)\wedge B$ 真，于是 $A(x)$和 B 都为真，所以 $\forall xA(x)$和 B 取真，因此 $\forall xA(x)\wedge B$ 真. 反过来，亦成立.

可借助下面的例子帮助理解上述 4 个等值式. 例中 D 表示班上所有的同学，$A(x)$：x 来上课了，B：小帅是班长.

【例 4-13】 证明下列与蕴涵联结词有关的 4 个等值式，其中 B 中不含自由变元 x.

(1) $\forall x(A(x)\rightarrow B)=\exists xA(x)\rightarrow B$.

(2) $\forall x(B\rightarrow A(x))=B\rightarrow \forall xA(x)$.

(3) $\exists x(A(x)\rightarrow B)=\forall xA(x)\rightarrow B$.

(4) $\exists x(B\rightarrow A(x))=B\rightarrow \exists xA(x)$.

证 只证(1)和(2)，其余留作练习.

$$\begin{aligned}\forall x(A(x)\rightarrow B)&=\forall x(\neg A(x)\vee B)=\forall x\neg A(x)\vee B\\&=\neg\exists xA(x)\vee B=\exists xA(x)\rightarrow B\end{aligned}$$

$$\forall x(B\rightarrow A(x))=\forall x(\neg B\vee A(x))=\neg B\vee\forall xA(x)=B\rightarrow\forall xA(x)$$

3. 量词分配律

(1) $\forall x(A(x)\wedge B(x))=\forall xA(x)\wedge\forall xB(x)$.

(2) $\exists x(A(x)\vee B(x))=\exists xA(x)\vee\exists xB(x)$.

首先注意，$\forall$ 对 $\wedge$ 可分配，但 $\forall x(A(x)\vee B(x))\neq\forall xA(x)\vee\forall xB(x)$，例如若令 $D=\mathbf{Z}$，$A(x)$：x 是偶数，$B(x)$：x 是奇数，则 $\forall x(A(x)\vee B(x))$在上述解释下取真，而 $\forall xA(x)\vee\forall xB(x)$在上述解释下取假.

同样，$\exists$ 对 $\vee$ 可分配，但 $\exists x(A(x)\wedge B(x))\neq\exists xA(x)\wedge\exists xB(x)$，例子同上.

(1)的证明：任意给定个体域 D 上的解释 I，若 $\forall x(A(x)\wedge B(x))$在解释 I 取真，则任意 $d\in D$，$A(d)\wedge B(d)$取真，进而 $A(d)$和 $B(d)$都为真，于是 $\forall xA(x)$及 $\forall xB(x)$为真，所以 $\forall xA(x)\wedge\forall xB(x)$取真. 反过来，若 $\forall xA(x)\wedge\forall xB(x)$在解释 I 取真，则同样有 $\forall x(A(x)\wedge B(x))$为真.

(2)留作练习.

下述例子对记住(1)和(2)是有帮助的：令 $D=\{$全班同学$\}$，$A(x)$：x 会唱歌，$B(x)$：x 会跳舞.

4. 双重量词

(1) $\forall x\forall yA(x,y)=\forall y\forall xA(x,y)$.

(2) $\exists x\exists yA(x,y)=\exists y\exists xA(x,y)$.

显然，(1)和(2)是成立的. 例如，用 D 表示一些直线组成的集合，$A(x,y)$表示 x 平行于 y，这时(1)和(2)左右两边的含义是相同的. 需再次提醒注意，$\forall x\exists yA(x,y)\neq\exists y\forall xA(x,y)$.

【例 4-14】 证明 $\forall x\forall y(A(x)\rightarrow B(y))=\exists xA(x)\rightarrow\forall yB(y)$.

证

$$\begin{aligned}&\forall x\forall y(A(x)\rightarrow B(y))=\forall x\forall y(\neg A(x)\vee B(y))\\&=\forall x(\forall y(\neg A(x)\vee B(y)))=\forall x(\neg A(x)\vee\forall yB(y))\\&=\forall x\neg A(x)\vee\forall yB(y)=\neg\exists xA(x)\vee\forall yB(y)\\&=\exists xA(x)\rightarrow\forall yB(y).\end{aligned}$$

最后要说明的是,等值置换定理在谓词逻辑中仍然成立.

习 题 4.4

1. 证明下列等值式.

(1) $\neg \forall x A(x) = \exists x \neg A(x)$.

(2) $\neg \exists x A(x) = \forall x \neg A(x)$.

2. 证明下列等值式,其中 B 中不含有自由变元 x.

(1) $\forall x(A(x) \vee B) = \forall x A(x) \vee B$.

(2) $\exists x(A(x) \wedge B) = \exists x A(x) \wedge B$.

(3) $\exists x(A(x) \vee B) = \exists x A(x) \vee B$.

3. 设 B 中不含自由变元 x,证明下列等值式.

(1) $\exists x(A(x) \rightarrow B) = \forall x A(x) \rightarrow B$.

(2) $\exists x(B \rightarrow A(x)) = B \rightarrow \exists x A(x)$.

4. 证明等值式 $\exists x(A(x) \vee B(x)) = \exists x A(x) \vee \exists x B(x)$.

5. 证明等值式 $\exists x(A(x) \rightarrow B(x)) = \forall x A(x) \rightarrow \exists x B(x)$.

6. 证明下列等值式.

(1) $\forall x \forall y(A(x) \vee B(y)) = \forall x A(x) \vee \forall y B(y)$.

(2) $\exists x \exists y(A(x) \wedge B(y)) = \exists x A(x) \wedge \exists y B(y)$.

(3) $\exists x \exists y(A(x) \rightarrow B(y)) = \forall x A(x) \rightarrow \exists y B(y)$.

7. 在谓词逻辑中,下列各谓词公式哪些是永真式?给出理由.

(1) $\exists x(A(x) \vee B(x)) \leftrightarrow \exists x A(x) \vee \exists x B(x)$.

(2) $\neg \exists x A(x) \wedge \forall x B(x) \leftrightarrow \forall x(\neg A(x) \wedge B(x))$.

(3) $\exists x(A(x) \rightarrow B(x)) \leftrightarrow (\forall x A(x) \rightarrow \exists x B(x))$.

(4) $\exists x \exists y(A(x) \rightarrow B(y)) \leftrightarrow (\forall x A(x) \rightarrow \exists y B(y))$.

8. 以下等值式是否成立,为什么?

(1) $\exists x(A(x) \rightarrow B(x)) = \forall x A(x) \rightarrow \exists x B(x)$.

(2) $\exists x(A(x) \rightarrow \forall x B(x)) = \forall x A(x) \rightarrow \forall x B(x)$.

4.5 谓词公式的前束范式

讨论谓词公式的标准形式是很有意义的.

本节讨论谓词公式的前束范式.实际上,在前束范式的基础上,可以进一步得出谓词公式的 Skolem 范式[12],进而得出一个谓词公式永真(假)在有限步内可判定的著名结论.

4.5.1 谓词公式的前束范式的定义

【定义 4-4】 设 A 是谓词公式,若 $A = Q_1 x_1 Q_2 x_2 \cdots Q_n x_n(\cdots B \cdots)(n \geqslant 0)$,其中 Q_i 为 $\forall$ 或 $\exists$,B 中不含量词,则称 $Q_1 x_1 Q_2 x_2 \cdots Q_n x_n(\cdots B \cdots)$ 为 A 的**前束范式**(prenex normal form).

直观地理解，谓词公式的前束范式是将所有量词放在最前面，去作用整个 B. 特别注意，若 $A=\forall xP(x)\to Q(x,y)$ 不是 A 的前束范式，因为尽管 $\forall x$ 在最前面，但它的辖域是 $P(x)$.

当 $n=0$ 时，即 A 中无量词，则 A 也是前束范式.

显然，谓词公式 A 与其前束范式是等值的.

4.5.2 谓词公式的前束范式的计算

前束范式的计算步骤如下.

(1) 将逻辑联结词归约到只含 $\neg,\wedge,\vee$ 的谓词公式.

因为在要求记住的谓词逻辑等值式中，没有出现除 $\neg,\wedge,\vee$ 外的其他联结词.

(2) 使用以下两个等值式将否定联结词往里面移.

① $\neg\forall xA(x)=\exists x\neg A(x)$.

② $\neg\exists xA(x)=\forall x\neg A(x)$.

(3) 使用等值式将所有量词移到最前面，必要时使用改名技巧.

【例 4-15】 求 $\forall xA(x)\wedge\forall xB(x)$ 的前束范式.

解 $\forall xA(x)\wedge\forall xB(x)=\forall x(A(x)\wedge B(x))$

【例 4-16】 求 $\forall xA(x)\to\exists xB(x)$ 的前束范式.

解 $\forall xA(x)\to\exists xB(x)=\neg\forall xA(x)\vee\exists xB(x)$

$=\exists x\neg A(x)\vee\exists xB(x)=\exists x(\neg A(x)\vee B(x))$

【例 4-17】 求 $\exists xA(x)\wedge\exists xB(x)$ 的前束范式.

解 $\exists xA(x)\wedge\exists xB(x)=\exists xA(x)\wedge\exists yB(y)$

$=\exists x(A(x)\wedge\exists yB(y))=\exists x\exists y(A(x)\wedge B(y))$

直接求 $\exists xA(x)\wedge\exists xB(x)$ 的前束范式没有等值式可用，采用改名的技巧就可以利用等值式了，但要求前束范式中的量词要尽可能地少.

【例 4-18】 求 $\exists xF(y,x)\to\forall yG(y)$ 的前束范式.

解 $\exists xF(y,x)\to\forall yG(y)=\neg\exists xF(y,x)\vee\forall yG(y)$

$=\forall x\neg F(y,x)\vee\forall yG(y)=\forall x(\neg F(y,x)\vee\forall yG(y))$

$=\forall x(\neg F(t,x)\vee\forall yG(y))$（对自由变元 y 改名）

$=\forall x\forall y(\neg F(t,x)\vee G(y))$.

习 题 4.5

1. 判断下列谓词公式是否是前束范式.

(1) $B\to\forall xA(x)$.

(2) $\forall xA(x)\to B$.

(3) $\forall x(A(x)\to B)$.

(4) $\forall x(A(x)\to\exists yB(y))$.

(5) $A(x)\to B$.

2. 求下列谓词公式的前束范式.

(1) $\forall x(A(x)\to\exists yB(x,y))$.

(2) $\exists x(\neg\exists yP(x,y)\to(\exists zQ(z)\to R(x)))$.

(3) $\neg(\forall xA(x)\to\exists y\forall zB(y,z))$.

(4) $\exists xA(x)\vee\exists xB(x)\to\exists x(A(x)\vee B(x))$.

3. 求下列谓词公式的前束范式.

(1) $(\neg\exists xA(x)\vee\forall yB(y))\wedge(A(x)\to\forall zC(z))$.

(2) $\forall x(A(x)\to(\exists zB(z)\to\exists yC(x,y)))$.

(3) $\forall x(\forall y\exists zA(x,y,z)\to\exists z\forall u(B(x,z)\vee C(x,u,z)))$.

(4) $\forall x\forall y(\exists zA(x,y,z)\wedge\exists uB(x,u)\to\exists vB(y,v))$.

4.6 谓词逻辑中的推理

4.6.1 逻辑蕴涵式

设 $H_1,H_2,\cdots,H_n$ 和 C 是谓词公式,$H_1,H_2,\cdots,H_n\Rightarrow C$ 的含义同上章 3.7 节.

显然,$H_1,H_2,\cdots,H_n\Rightarrow C$ 的充要条件是 $H_1\wedge H_2\wedge\cdots\wedge H_n\to C$ 是永真式.

首先,根据命题逻辑中的逻辑蕴涵式可以产生谓词逻辑的逻辑蕴涵式.如在命题逻辑中有 $p\to q,p\Rightarrow q$,则$(p\to q)\wedge p\to q$ 永真,对于谓词公式 A 和 B,$(A\to B)\wedge A\to B$ 永真,从而有 $A\to B,A\Rightarrow B$.

其次,可以得出与量词有关的一些逻辑蕴涵式.

【例 4-19】 证明 $\forall xA(x)\Rightarrow A(t)$.

证 因为由 4.3 节例 4-9 知,$\forall xA(x)\to A(t)$永真.

【例 4-20】 证明 $\exists x\forall yA(x,y)\Rightarrow\forall y\exists xA(x,y)$.

证 任意给定个体域 D 上的解释 I,假定 $\exists x\forall yA(x,y)$在解释 I 下取真,则存在 $d_0\in D$,对于任意 $d\in D$,均有 $A(d_0,d)$取真,于是 $\forall y\exists xA(x,y)$在解释 I 下取真,从而 $\exists x\forall yA(x,y)\Rightarrow\forall y\exists xA(x,y)$.

【例 4-21】 证明 $\exists y\forall xA(x,y)$不是 $\forall x\exists yA(x,y)$的有效结论.

证 设个体域 $D=\mathbf{R}$,$A(x,y)$:$x>y+3$,则 $\forall x\exists yA(x,y)$表示"对于任意实数 x,均存在实数 y,使得 $x>y+3$",它是真命题,而 $\exists y\forall xA(x,y)$表示"存在实数 y,对于任意实数 x,都有 $x>y+3$",它是假命题,所以 $\forall x\exists yA(x,y)\to\exists y\forall xA(x,y)$不是永真式,因此 $\exists y\forall xA(x,y)$不是 $\forall x\exists yA(x,y)$的有效结论.

4.6.2 基本推理规则

命题逻辑中的基本推理规则可以很方便地推广到谓词逻辑,参见上章 3.7 节.

谓词逻辑中有两个非常重要与量词有关的逻辑蕴涵式.

【定理 4-1】 下列逻辑蕴涵式成立:

(1) $\forall xA(x)\vee\forall xB(x)\Rightarrow\forall x(A(x)\vee B(x))$.

(2) $\exists x(A(x)\wedge B(x))\Rightarrow\exists xA(x)\wedge\exists xB(x)$.

证 只证(2),(1)留作练习.

任意给定个体域 D 上的解释 I,假定 $\exists x(A(x)\wedge B(x))$ 在解释 I 下取真,则存在 $d_0\in D$,使得 $A(d_0)\wedge B(d_0)$ 为真,这时 $A(d_0)$ 和 $B(d_0)$ 为真,进而 $\exists xA(x)$ 及 $\exists xB(x)$ 在解释 I 下取真,(2)得证.

同样,下述例子对记住(1)和(2)是有益的:令 $D=\{$全班同学$\}$,$A(x)$:x 会唱歌,$B(x)$:x 会跳舞.

【例 4-22】 证明或反驳下列结论.

(1) $\neg\forall xA(x)\Rightarrow\forall x\neg A(x)$.

(2) $\exists x(A(x)\rightarrow B(x))\Rightarrow\exists xA(x)\rightarrow\exists xB(x)$.

解 (1) 因为 $\neg\forall xA(x)=\exists x\neg A(x)$,而显然 $\exists x\neg A(x)$ 不能推出 $\forall x\neg A(x)$. 例如,设个体域 $D=\mathbf{Z}$, $A(x)$:x 是偶数,则 $\forall xA(x)$ 是假命题,从而 $\neg\forall xA(x)$ 是真命题,而 $\forall x\neg A(x)$ 表示"任意整数都不是偶数",它是假命题,因此结论 $\neg\forall xA(x)\Rightarrow\forall x\neg A(x)$ 不成立.

(2) 不成立. 例如,令个体域 $D=\{1,2\}$,$\dfrac{A(1)}{1}$,$\dfrac{A(2)}{0}$,$\dfrac{B(1)}{0}$,$\dfrac{B(2)}{0}$,这时因为 $A(2)\rightarrow B(2)$ 为真,于是 $\exists x(A(x)\rightarrow B(x))$ 是真命题,而 $A(1)$ 为真,即 $\exists xA(x)$ 为真,但 $\exists xB(x)$ 取假,所以 $\exists xA(x)\rightarrow\exists xB(x)$ 在上述解释下为假,故(2)不成立.

4.6.3 谓词逻辑的自然推理系统

谓词逻辑的自然推理系统是命题逻辑的自然推理系统的一种推广. 初始符号增加了函词、谓词、量词;谓词公式的形成规则参见 4.2 节谓词公式的定义;没有公理;基本推理规则增加定理 4-1 中两个逻辑蕴涵式,以及下述 4 个与量词有关的基本推理规则.

我们以最简洁的方式加以介绍.

1. 全称量词消去(Universal quantifier Specification, US)规则

(1) $\forall xA(x)$.

(2) $A(c)$(其中 c 为个体域中任意个体).

2. 全称量词产生(Universal quantifier Generalization, UG)规则

(1) $A(c)$(其中 c 为个体域中任意个体).

(2) $\forall xA(x)$.

3. 存在量词消去(Existential quantifier Specification, ES)规则

(1) $\exists xA(x)$.

(2) $A(c)$(其中 c 为个体域中某个体,c 在其前面原则上未出现过).

注意 由 $\exists xA(x)$ 推出 $A(c)$,要确保 c 与其他自由变元无关,参见例 4-27.

4. 存在量词产生(Existential quantifier Generalization, EG)规则

(1) $A(c)$(其中 c 为个体域中某个体).

(2) $\exists xA(x)$.

【例 4-23】 证明苏格拉底三段论推理的有效性.

证 用 s:苏格拉底,$P(x)$:x 是人,$D(x)$:x 是要死的,则

$$\forall x(P(x)\rightarrow D(x)),P(s)\Rightarrow D(s)$$

(1) $P(s)$　　P

(2) $\forall x(P(x)\rightarrow D(x))$　　P

(3) $P(s)\rightarrow D(s)$　　US(2)

(4) $D(s)$　　T(1)(3)I

【例 4-24】 用构造法证明以下推理：

$$\forall x(F(x)\rightarrow G(x)),\exists xF(x)\Rightarrow\exists xG(x)$$

证

(1) $\exists xF(x)$　　P

(2) $F(c)$　　ES(1)

(3) $\forall x(F(x)\rightarrow G(x))$　　P

(4) $F(c)\rightarrow G(c)$　　US(3)

(5) $G(c)$　　T(2)(4)I

(6) $\exists xG(x)$　　EG(5)

注意 (1)、(2)与(3)、(4)的顺序不能颠倒.(2)中 $F(c)$ 中的 c 是某个体,(4)中 $F(c)\rightarrow G(c)$ 中的 c 本来是任意个体,现取为(2)中出现的 c,这是可以的.但反过来就不行.

避免这种错误的最好方法是像上面的证明过程一样,先消去存在量词,再消去全称量词.

【例 4-25】 用构造法证明以下推理：

$$\neg\exists x(F(x)\land H(x)),\forall x(G(x)\rightarrow H(x))\Rightarrow\forall x(G(x)\rightarrow\neg F(x))$$

证

(1) $\neg\exists x(F(x)\land H(x))$　　P

(2) $\forall x(\neg F(x)\lor\neg H(x))$　　T(1)E

(3) $\neg F(c)\lor\neg H(c)$　　US(2)

(4) $H(c)\rightarrow\neg F(c)$　　T(3)E

(5) $\forall x(G(x)\rightarrow H(x))$　　P

(6) $G(c)\rightarrow H(c)$　　US(5)

(7) $G(c)\rightarrow\neg F(c)$　　T(4)(6)I

(8) $\forall x(G(x)\rightarrow\neg F(x))$　　UG(7)

【例 4-26】 设个体域 D 为所有人组成的集合,在谓词逻辑中符号化下列各命题,并用构造法证明以下推理：每位科学家都是勤奋的,每个勤奋且身体健康的人在事业上都会获得成功,存在身体健康的科学家,所以存在事业获得成功或事业半途而废的人.

解 令 $Q(x)$：x 是勤奋的,$H(x)$：x 是健康的,$S(x)$：x 是科学家,$C(x)$：x 是事业获得成功的人,$F(x)$：x 是事业半途而废的人,则

$$\forall x(S(x)\rightarrow Q(x)),\forall x(Q(x)\land H(x)\rightarrow C(x)),\exists x(S(x)\land H(x))$$
$$\Rightarrow\exists x(C(x)\lor F(x))$$

(1) $\exists x(S(x)\land H(x))$　　P

(2) $S(c)\land H(c)$　　ES(1)

(3) $S(c)$　　T(2)I

(4) $H(c)$　　T(2)I

(5) $\forall x(S(x)\rightarrow Q(x))$ P

(6) $S(c)\rightarrow Q(c)$ US(5)

(7) $Q(c)$ T(3)(6)I

(8) $Q(c)\wedge H(c)$ T(4)(7)I

(9) $\forall x(Q(x)\wedge H(x)\rightarrow C(x))$ P

(10) $Q(c)\wedge H(c)\rightarrow C(c)$ US(9)

(11) $C(c)$ T(8)(10)I

(12) $C(c)\vee F(c)$ T(11)I

(13) $\exists x(C(x)\vee F(x))$ EG(12)

关于多重量词的推理,需要注意的问题比较多,请参阅有关文献[14].

【例 4-27】 指出下列推理步骤中的错误.

(1) $\forall x\exists y(x>y)$ P

(2) $\exists y(c>y)$ US(1)

(3) $c>d$ ES(2)

(4) $\forall x(x>d)$ UG(3)

(5) $\exists y\forall x(x>y)$ EG(4)

解 (3)错.在(2)中的 c 是个体域中任意个体,实际上是自由变元,当由(2)消去存在量词 $\exists y$ 时,不能利用 ES 规则.换句话说,(3)中所得到的 d 与 c 密切相关.

已经有例子表明,$\forall x\exists yA(x,y)\rightarrow\exists y\forall xA(x,y)$不是永真式.

习 题 4.6

1. 证明 $\forall xA(x)\Rightarrow\exists xA(x)$.
2. 证明 $\exists x\forall yA(x,y)\Rightarrow\exists x\exists yA(x,y)$.
3. 证明 $\forall xA(x)\vee\forall xB(x)\Rightarrow\forall x(A(x)\vee B(x))$.
4. 证明 $\exists xA(x)\rightarrow\forall xB(x)\Rightarrow\forall x(A(x)\rightarrow B(x))$.
5. 试判断下列谓词公式是否为永真式,给出理由.

(1) $\forall x(A(x)\vee B(x))\rightarrow\forall xA(x)\vee\forall xB(x)$.

(2) $\exists xA(x)\wedge\exists xB(x)\rightarrow\exists x(A(x)\wedge B(x))$.

6. 证明或反驳下列结论.

(1) $\exists x(\neg A(x)\rightarrow B(x))\rightarrow\forall xC(x)\Rightarrow\forall x(B(x)\rightarrow C(x))$.

(2) $\exists x(A(x)\rightarrow\forall yB(x,y))\Rightarrow\neg\forall y\exists xB(x,y)\rightarrow\forall xA(x)$.

7. 构造下列推理的证明:

$$\forall x(F(x)\rightarrow G(x)),\forall x(R(x)\rightarrow\neg G(x))\Rightarrow\forall x(R(x)\rightarrow\neg F(x)).$$

8. 构造下列推理的证明:$\forall x(S(x)\wedge W(x)),\exists xY(x)\Rightarrow\exists x(S(x)\wedge Y(x))$.
9. 使用反证法,构造下列推理的证明:

$$\forall x(A(x)\rightarrow\neg B(x)),\forall x(B(x)\vee C(x)),\neg\forall xC(x)\Rightarrow\neg\forall xA(x)$$

10. 使用 CP 规则,构造下列推理的证明:

$$\exists xE(x)\rightarrow\forall x(Q(x)\rightarrow F(x)),\exists xS(x)\rightarrow\exists xQ(x)$$

$\Rightarrow \exists x(E(x) \wedge S(x)) \rightarrow \exists x F(x)$

11. 证明下列推理的有效性：所有有理数是实数，某些有理数是整数，所以某些实数是整数.

12. 构造下列推理的证明：自然数都是整数，整数都是有理数，有些有理数不是整数，所以自然数都是有理数，并且存在既不是自然数又不是整数的有理数.

13. 在谓词逻辑中符号化下列命题，并用构造法证明以下推理的有效性：

所有牛都有角，有些动物是牛，所以有些动物有角.

14. 在谓词逻辑中符号化下列命题，并用构造法证明以下推理的有效性：

鸟会飞，猴子不会飞，所以猴子不是鸟.

15. 假定个体域为所有人组成的集合，在谓词逻辑中符号化下列命题，并用构造法证明以下推理的有效性：

每个学生或是勤奋的或是聪明的，所有勤奋的人都会有所作为，并非每个学生都有所作为，所以有些学生是聪明的.

16. 在谓词逻辑中符号化下列命题，并用构造法证明以下推理的有效性：

桌上的每本书都是杰作，写出杰作的人都是天才，某个不出名的人写了桌上的某本书，所以某个不出名的人是天才.

本 章 小 结

1. 个体、谓词、量词和函词

对原子命题内部结构及其逻辑关系进行讨论就是谓词逻辑，这些讨论涉及集合、映射、运算和关系. 命题的考虑对象称为个体，个体所在的范围称为个体域.

表示个体性质以及个体之间关系的词称为谓词. 对于 $n(n\geqslant 1)$ 元谓词 P，$P(x_1,x_2,\cdots,x_n)$ 是命题函数.

常用的量词有全称量词 $\forall$ 和存在量词 $\exists$. 全称量词 $\forall$ 相当于“任意”、“全部”、“所有”、“每一个”、“一切”等，存在量词 $\exists$ 相当于“有些”、“某些”、“有的”、“存在”、“至少有一个”等. 量词 $\forall x$ 或 $\exists x$ 的作用或管辖的范围称为 $\forall x$ 或 $\exists x$ 的作用域或辖域，辖域内的个体变元 x 称为约束变元. 不受任何量词约束的变元称为自由变元.

表示个体之间的函数关系就是函词.

重点掌握量词的辖域，能区分约束变元和自由变元.

2. 谓词公式及命题的符号化.

使用谓词将命题符号化得到的含义正确的表达式就是谓词公式. 要求能熟练在谓词逻辑中将命题符号化，具体步骤：

第 1 步　找出所给命题中的所有个体常量，并用 $a,b,c,\cdots,a_i,b_i,c_i,\cdots$ 表示(必要时使用函数表示).

第 2 步　首先确定在给定个体域中应该选用的所有谓词，特别注意特性谓词的选取；其次确定量词.

第 3 步　确定函词.

第 4 步　通过找出联结词，将所给命题符号化.

3. 谓词公式的解释及类型

了解谓词公式的解释 I：

(1) 指定个体域 D.

(2) 对于谓词公式中的命题变元指派其真值.

(3) 对于谓词公式中的个体常量及其自由变元解释为指定个体域 D 中的元素.

(4) 对于谓词公式中的函词解释为 D 上的函数.

(5) 对于谓词公式中的谓词解释为 D 上的谓词.

会计算谓词公式在给定解释 I 下的真值.

在任何解释下均为真的谓词公式称为永真式或有效式. 至少存在一种解释使其为 1 的谓词公式称为可满足式,否则称为不可满足式或矛盾式或永假式. 既存在取 1 的解释,又存在取 0 的解释的谓词公式称为中性式或偶然式.

4. 逻辑等值的谓词公式

设 A,B 是谓词公式,$A=B$ 是指 A 和 B 在任何解释下的取值都相同.

记住 10 个基本谓词公式等值式，特别是下面两个较难记住的等值式：

(1) $\forall x(A(x)\wedge B(x))=\forall xA(x)\wedge\forall xB(x)$.

(2) $\exists x(A(x)\vee B(x))=\exists xA(x)\vee\exists xB(x)$.

5. 谓词公式的前束范式

设 A 是谓词公式,若 $A=Q_1x_1Q_2x_2\cdots Q_nx_n(\cdots B\cdots)(n\geqslant 0)$,其中 Q_i 为 $\forall$或 $\exists$,B 中不含量词,则称 $Q_1x_1Q_2x_2\cdots Q_nx_n(\cdots B\cdots)$为 A 的前束范式.

要求熟练掌握谓词公式前束范式的计算，计算步骤如下：

第 1 步　将逻辑联结词归约到只含 $\neg,\wedge,\vee$ 的谓词公式.

第 2 步　使用以下两个等值式将否定联结词往里面移.

(1) $\neg\forall xA(x)=\exists x\neg A(x)$.

(2) $\neg\exists xA(x)=\forall x\neg A(x)$.

第 3 步　使用基本谓词公式等值式将所有量词移到最前面,必要时使用改名技巧.

6. 谓词逻辑中的推理

要求能对较简单的谓词逻辑中推理有效性进行构造性证明.

重要的两个谓词逻辑蕴涵式：

(1) $\forall xA(x)\vee\forall xB(x)\Rightarrow\forall x(A(x)\vee B(x))$.

(2) $\exists x(A(x)\wedge B(x))\Rightarrow\exists xA(x)\wedge\exists xB(x)$.

4 个与量词有关的基本推理规则：

Ⅰ. US 规则：全称量词消去规则.

(1) $\forall xA(x)$.

(2) $A(c)$(其中 c 为个体域中任意个体).

Ⅱ. UG：全称量词产生规则.

(1) $A(c)$(其中 c 为个体域中任意个体).

(2) $\forall xA(x)$.

Ⅲ．ES 规则：存在量词消去规则．

（1）$\exists xA(x)$．

（2）$A(c)$（其中 c 为个体域中某个体，c 在其前面原则上未出现过）．

Ⅳ．EG 规则：存在量词产生规则．

（1）$A(c)$（其中 c 为个体域中某个体）．

（2）$\exists xA(x)$．

第 5 章 代数结构

接下来将介绍代数结构的一般内容以及常见的几种代数结构，它是一种用代数方法建立的数学模型.

代数结构简称代数，它是**抽象代数**(abstract algebra)或**近世代数**(modern algebra)，不是初等代数，也不是高等代数，它始于 19 世纪初，形成于 20 世纪 30 年代，在这期间，挪威数学家 N. H. Abel、法国数学家 E. Galois、英国数学家 A. De Morgan 和 G. Boole 等人都做出了杰出的贡献.

代数结构研究由一般元素(不仅仅是数字、符号等)组成的集合上的运算，以及运算满足一些给定性质的数学结构的性质.

代数结构在计算机科学中起着重要作用，前面几章分别讨论的是集合代数、关系代数和逻辑代数. 实际上，计算机系统本身就是一种代数结构. 众所周知，利用布尔代数可进行逻辑电路设计的分析和优化. 利用代数结构可研究抽象数据结构的性质与操作，它也是程序设计语言的理论基础.

在本章讲解的群、环、域是根据运算及其所满足的性质按“代数结构”进行分类的，格和布尔代数是根据“序结构”进行的讨论，它们在组合计数、代数编码理论、形式语言与自动机理论等学科中都发挥了重要作用. 同时，代数结构的研究采用的是形式化方法，对于培养大家的抽象思维和计算思维能力是非常有用的.

5.1 代数结构简介

5.1.1 代数结构的定义

“代数”总是与运算联系在一起的，如代数式、代数和、代数方程以及代数数等. 先给出代数的定义.

【定义 5-1】 设 A 是非空集合，$f_1, f_2, \cdots, f_k(k\geqslant 1)$是 A 上的代数(封闭)运算，则集合 A 连同其上的代数运算 $f_1, f_2, \cdots, f_k$ 称为**代数结构**(algebra structure)或**代数系统**(algebra system)或简称**代数**(algebra)，记为$(A, f_1, f_2, \cdots, f_k)$，在已知运算 $f_1, f_2, \cdots, f_k$ 的情况下可简记为 A.

对于代数结构$(A, f_1, f_2, \cdots, f_k)$的理解，需注意以下几点：

(1) $A\neq\varnothing$.

(2) $f_1, f_2, \cdots, f_k(k\geqslant 1)$是 A 上的代数(封闭)运算(参见第 1 章 1.3 节).

(3) 运算 $f_1, f_2, \cdots, f_k$ 在代数结构中是有顺序的. 实际上，代数结构$(A, f_1, f_2, \cdots, f_k)$是一个$(k+1)$元组.

(4) 运算 f_i 的元数 $n_i(1\leqslant i\leqslant k)$可以相同，也可以不同.

【例 5-1】 验证下列集合及其上的运算构成代数结构.

(1) 实数集合 **R** 关于实数的加法运算“+”:(**R**, +).

(2) 实数集合 **R** 关于实数的加法运算“+”和实数的乘法运算“·”:(**R**, +, ·).

(3) 集合 X 的幂集 $P(X)$ 关于集合的并“∪”运算、集合的交“∩”运算和集合的补运算“$^{-}$”:$(P(X), \cup, \cap, ^{-})$.

解 根据代数结构的定义很容易验证(略).

【定义 5-2】 $(A, f_1, f_2, \cdots, f_k)$是代数结构,若 A 是有限集合,则$(A, f_1, f_2, \cdots, f_k)$是**有限代数结构**,否则称为**无限代数结构**.

在例 5-1 中,(1)和(2)中的代数结构是无限代数结构. 在(3)中,若 X 是有限集合,则$(P(X), \cup, \cap, ^{-})$是有限代数结构;若 X 是无限集合,则$(P(X), \cup, \cap, ^{-})$是无限代数结构.

5.1.2 两种最简单的代数结构:半群及独异点

下面介绍两种最简单的代数结构.

【定义 5-3】 设 $*$ 是非空集合 S 上的 2 元代数运算,若 $*$ 满足结合律,即对于任意 $x, y, z \in S$,有$(x * y) * z = x * (y * z)$,则称$(S, *)$是**半群**(semigroup).

虽然,实数集合 **R** 关于其上的乘法运算“·”作成一个半群(**R**, ·).

下面的半群在计算机科学的研究中有着重要的作用.

【例 5-2】 设 Σ 是若干个字母组成的集合,称为字母表,由 Σ 中有限个字母组成的序列称为 Σ 上的串,不含任何字母的串称为空串,记为 λ. 令 Σ^* 是所有 Σ 上的串组成的集合,其上的运算为 Σ^* 上的连接运算“$\circ$”.

任意 $\alpha = s_1 s_2 \cdots s_k \in \Sigma^*$, $\beta = t_1 t_2 \cdots t_s \in \Sigma^*$,有 $\alpha \circ \beta = s_1 s_2 \cdots s_k t_1 t_2 \cdots t_s$,很容易验证:$(\Sigma^*, \circ)$是半群.

实际上,Σ 上的所有非空串组成的集合 Σ^+,关于其上的串的连接运算$\circ$也构成一个半群$(\Sigma^+, \circ)$.

设 $\omega = s_1 s_2 \cdots s_k \in \Sigma^*$,则称串 ω 的长度为 k,记为$|\omega| = k$. 显然,若$|\alpha| = k$, $|\beta| = s$,则$|\alpha \circ \beta| = k + s$.

【定义 5-4】 设 $*$ 是非空集合 M 上的 2 元代数运算,若 $*$ 满足结合律且 M 关于 $*$ 有幺元 e,即对于任意 $x \in M$,有 $x * e = e * x = x$,则称$(M, *, e)$为**独异点**(monoid),其中幺元 e 是一个独特、奇异的元素.

【例 5-3】 在例 5-3 中,$(\Sigma^*, \circ, \lambda)$是独异点,而$(\Sigma^+, \circ)$不是.

注意

(1) 在$(\Sigma^*, \circ, \lambda)$中的 λ 称为**代数常数**. 代数结构中的代数常数可以不止一个,例如在后面将学习的布尔代数就有 2 个代数常数. 当然也可以没有代数常数.

(2) $(\Sigma^*, \circ)$是半群,$(\Sigma^*, \circ, \lambda)$是独异点,它们是两个不同的代数结构. 正因为这样,一个最好的处理方式是将代数常数看作是 0 元运算,$(\Sigma^*, \circ, \lambda)$有 1 个 0 元运算(及 1 个二元运算),布尔代数有 2 个 0 元运算.

因为半群中的 $*$ 运算满足结合律,可以定义元素 a 的正整数方幂 a^n(n 为正整数)如下:

$$a^1 = a;$$

$$a^n = \overbrace{a * a * \cdots * a}^{n个}(n \geqslant 2)$$

注意 元素 a 的正整数方幂 a^n 是对任意具有结合性的运算都可以定义.对于实数集合 $\mathbf{R}$ 上的乘法运算,很容易理解;对于实数集合 $\mathbf{R}$ 上的加法运算+,$a^n=\overbrace{a+a+\cdots+a}^{n个}=na$.

显然对于正整数 m 和 n,有下面的结论:

(1) $a^m * a^n = a^{m+n}$;

(2) $(a^m)^n = a^{mn}$.

因为 $*$ 运算是 S 上的封闭运算,所以对于 $a\in S$,有 $a^n\in S$(n 为正整数).

由上述的半群和独异点这两个简单的代数结构可知,特殊的代数结构是将运算满足的条件作为公理进行定义的. 接下去的任务是从这些公理出发推导出一些有用的结论,它对于所有满足给定公理的代数系统都成立. 先看一个关于有限半群结论的推导方法,更多的特殊代数结构的结论的推导见后.

【例 5-4】 设$(S, *)$是有限半群,则$(S, *)$中存在幂等元素.

证 取 $a\in S$,显然对于任意正整数 n,有 $a^n\in S$. 因为 S 是有限集合,所以存在正整数 i 和 j(不妨设 $i>j$)使得 $a^i=a^j$.

令 $p=i-j>0$,显然有 $a^i=a^p * a^j$,即 $a^j=a^p * a^j$,进而有 $a^q=a^p * a^q$($\forall q\geqslant j$).

因为 $p\geqslant 1$,必存在正整数 k 满足 $kp\geqslant j$. 由上面的结论,有 $a^{kp}=a^p * a^{kp}$. 应用该结论 k 次,有

$$a^{kp} = a^p * a^{kp} = a^p * (a^p * a^{kp}) = a^{2p} * a^{kp} = \cdots = a^{kp} * a^{kp}.$$

令 $b=a^{kp}$,则 $b*b=b$,即 b 就是有限半群$(S, *)$的幂等元.

5.1.3 子代数

讨论代数结构,一种常用的方法是根据其子代数所具有的性质去推测原代数的性质.

【定义 5-5】 设$(A, f_1, f_2, \cdots, f_k)$是代数结构,$\varnothing\neq S\subseteq A$,若$(S, f_1, f_2, \cdots, f_k)$是代数结构,则称其为$(A, f_1, f_2, \cdots, f_k)$的**子代数**(subalgebra),可记为$(S, f_1, f_2, \cdots, f_k)\leqslant(A, f_1, f_2, \cdots, f_k)$. 在不强调运算情况下简称 S 是 A 的子代数,记为 $S\leqslant A$.

一般地,要验证 S 是否是 A 的子代数,只要验证 S 关于 A 中运算 $f_1, f_2, \cdots, f_k$ 是否封闭即可.

【例 5-5】 在例 5-1(2)中,有$(\mathbf{Z}, +, \cdot)$是$(\mathbf{R}, +, \cdot)$的子代数,因为整数集合 $\mathbf{Z}$ 关于加法运算和乘法运算是封闭的.

【例 5-6】 由本书第 1.3 节很容易知道,$(\mathbf{Z}_8, \cdot_8, 1)$是独异点,其中 $\mathbf{Z}_8=\{0, 1, 2, 3, 4, 5, 6, 7\}$, $\cdot_8$是模 8 的乘法运算. 取 $S=\{0,2,4\}$,这时 S 关于运算 $\cdot_8$是封闭的,但因为 $1\notin S$,即 S 关于 $\mathbf{Z}_8$中的 0 元运算不封闭,所以 S 不是 $\mathbf{Z}_8$的子代数.

5.1.4 代数结构的同态与同构

借助于映射(函数)可以讨论两个代数结构之间的关系.

为了讨论方便，先给出下面的定义.

【定义 5-6】 设$(A,f_1,f_2,\cdots,f_k)$和$(B,g_1,g_2,\cdots,g_k)$是代数结构，若 f_i 与 g_i 有相同的运算元数$(1\leqslant i\leqslant k)$，则称这两个代数结构是**同类型的**.

下面给出的是一般的两个代数结构同态的定义，针对具体的重要代数结构还会重新给出定义的.

【定义 5-7】 设$(A,f_1,f_2,\cdots,f_k)$和$(B,g_1,g_2,\cdots,g_k)$是同类型的代数结构，若存在 φ: $A\to B$ 且 φ 保持所有运算，即对于 n_i 元运算 f_i 和 $g_i(1\leqslant i\leqslant k)$，有

$$\varphi(f_i(x_1,x_2,\cdots,x_{n_i}))=g_i(\varphi(x_1),\varphi(x_2),\cdots,\varphi(x_{n_i})),\quad \forall x_1,x_2,\cdots,x_{n_i}\in A$$

即先(在 A 中)运算再映射等于先映射再(在 B 中)运算，则称 φ 为$(A,f_1,f_2,\cdots,f_k)$到$(B,g_1,g_2,\cdots,g_k)$的**同态映射**，称$(A,f_1,f_2,\cdots,f_k)$和$(B,g_1,g_2,\cdots,g_k)$**同态**(homomorphism).

请注意同态映射与同态的区别与联系，参见下面的两个例子.

【例 5-7】 对于代数结构$(\mathbf{Z},+,\cdot)$和$(\mathbf{Z}_m,+_m,\cdot_m)$(其运算参见例 1-17)，令 φ: $\mathbf{Z}\to\mathbf{Z}_m$，对于任意 $x\in\mathbf{Z}$，$\varphi(x)=x(\bmod m)$. 证明：φ 是$(\mathbf{Z},+,\cdot)$到$(\mathbf{Z}_m,+_m,\cdot_m)$的同态映射.

证 对于任意 $x,y\in\mathbf{Z}$，因为

$$\varphi(x+y)=(x+y)(\bmod m)=x(\bmod m)+_n y(\bmod m)=\varphi(x)+_m\varphi(y)$$

$$\varphi(x\cdot y)=(xy)(\bmod m)=x(\bmod m)\cdot_m y(\bmod m)=\varphi(x)\cdot_m\varphi(y)$$

所以，φ 是$(\mathbf{Z},+,\cdot)$到$(\mathbf{Z}_m,+_m,\cdot_m)$的同态映射.

【例 5-8】 证明：代数结构$(\Sigma^*,\circ,\lambda)$与$(\mathbf{N},+,0)$同态.

证 令 φ: $\Sigma^*\to\mathbf{N}$，对于任意 $x\in\Sigma^*$，$\varphi(x)=|x|$. 对于任意 $x,y\in\Sigma^*$，有

$$\varphi(x\circ y)=|x\circ y|=|x|+|y|=\varphi(x)+\varphi(y)$$

且 $\varphi(\lambda)=|\lambda|=0$，所以 φ 是$(\Sigma^*,\circ,\lambda)$到$(\mathbf{N},+,0)$的同态映射，于是$(\Sigma^*,\circ,\lambda)$与$(\mathbf{N},+,0)$同态.

同态一般用于模型简化. 下述定理说明了研究代数结构同态映射的必要性.

【定理 5-1】 设 φ 是代数结构$(A,f_1,f_2,\cdots,f_k)$到$(B,g_1,g_2,\cdots,g_k)$的同态映射，则$(\varphi(A),g_1,g_2,\cdots,g_k)$是$(B,g_1,g_2,\cdots,g_k)$的子代数，称$(\varphi(A),g_1,g_2,\cdots,g_k)$为同态映射 φ 的**同态像**.

证 显然，$\varphi(A)$关于运算 $g_1,g_2,\cdots,g_k$ 封闭，于是有 $\varphi(A)\leqslant B$.

定理 5-1 说明，同态像是$(A,f_1,f_2,\cdots,f_k)$在同态映射下的缩影，因此可以通过对较简单的同态像的性质的讨论去探测其原像$(A,f_1,f_2,\cdots,f_k)$的性质. 下面的例子可以进一步帮助理解同态像是如何对原代数结构进行缩影的.

【例 5-9】 很容易验证，代数结构$(\mathbf{Z},\cdot)$与$(B,*)$同态，其中“$\cdot$”是 $\mathbf{Z}$ 上的乘法运算，$B=\{$正,负,零$\}$，B 上的运算 $*$ 定义如表 5-1 所示.

表 5-1

*	正	负	零
正	正	负	零
负	负	正	零
零	零	零	零

解 定义 φ: $\mathbf{Z}\to B$ 如下，

$$\varphi(x)=\begin{cases}\text{正}, & x>0\\ \text{负}, & x<0\\ \text{零}, & x=0\end{cases}$$

对于任意 $x,y\in\mathbf{Z}$,有 $\varphi(x\cdot y)=\varphi(x)*\varphi(y)$,因此,代数结构$(\mathbf{Z},\cdot)$与$(B,*)$同态.

在例 5-9 中,$\varphi(\mathbf{Z})=B$ 将整数集合上乘法运算的特征完全表示出来了.

但请注意,两个同态的代数结构之间可能存在多个同态映射,请自己举例加以说明.

下面给出的是一般的两个代数结构(单同态、满同态)同构的定义.

【定义 5-8】 设 φ 是代数结构$(A,f_1,f_2,\cdots,f_k)$到$(B,g_1,g_2,\cdots,g_k)$的同态映射,

(1) 若 φ 是单射,则称 φ 为$(A,f_1,f_2,\cdots,f_k)$到$(B,g_1,g_2,\cdots,g_k)$的**单同态映射**.

(2) 若 φ 是满射,则称 φ 为$(A,f_1,f_2,\cdots,f_k)$到$(B,g_1,g_2,\cdots,g_k)$的**满同态映射**.

(3) 若 φ 是双射,则称 φ 为$(A,f_1,f_2,\cdots,f_k)$到$(B,g_1,g_2,\cdots,g_k)$的**同构映射**,称代数结构$(A,f_1,f_2,\cdots,f_k)$与$(B,g_1,g_2,\cdots,g_k)$**同构**(isomorphism),记为

$$(A,f_1,f_2,\cdots,f_k)\cong(B,g_1,g_2,\cdots,g_k)$$

由定义 5-8 知,两个同构的代数结构在本质上是完全相同的,所不同的仅仅是集合中的元素符号可能不同,其上的运算符号也可能不同,参见下面的例子.

【例 5-10】 设代数结构$(A,*)$和$(B,+)$分别如表 5-2 和表 5-3 所示.

表 5-2

$*$	a	b
a	a	b
b	b	a

表 5-3

+	偶	奇
偶	偶	奇
奇	奇	偶

很容易验证,$(A,*)\cong(B,+)$.

【定义 5-9】 设 φ 是代数结构$(A,f_1,f_2,\cdots,f_k)$到$(A,f_1,f_2,\cdots,f_k)$的同态(构)映射,则称 φ 是$(A,f_1,f_2,\cdots,f_k)$的**自同态(构)映射**.

习 题 5.1

1. 试举出 4 个代数结构的例子.

2. 对于表 5-4 给定的集合及其上定义的运算是否构成代数结构,在相应的位置填"√"(是)或"×"(否).

表 5-4

集合 \ 运算	+	−	·	$\lvert x-y\rvert$	$\lvert x\rvert$	max	min
$\mathbf{Z}$							
$\mathbf{N}$							
$\{x\mid 0\leqslant x\leqslant 10\}$							
$\{x\mid \lvert x\rvert\leqslant 5\}$							
$\{2x\mid x\in\mathbf{Z}\}$							

3. 设$(S,*)$是半群,$a\in S$,在 S 上定义运算$\circ$如下:

$$\forall x,y\in S, x\circ y=x*a*y$$

证明：$(S,\circ)$是半群.

4. 证明：$(\mathbf{Z}_n, \cdot_n, 1)$是独异点.

5. 分别给出子半群及子独异点的定义.

6. 设 φ 是仅一个 2 元运算代数结构$(A, *)$到$(B,\circ)$的同态映射，则

(1) 若 $*$ 在 A 中可交换，则$\circ$在 $\varphi(A)$中可交换.

(2) 若 $*$ 在 A 中有零元 θ，则$\circ$在 $\varphi(A)$中有零元 $\varphi(\theta)$.

7. 证明：正实数集合 $\mathbf{R}^+$ 关于乘法运算 · 所构成的代数结构$(\mathbf{R}^+, \cdot)$与实数集合 $\mathbf{R}$ 关于加法运算＋所构成的代数结构$(\mathbf{R}, +)$同构.

8. 非零实数集合 $\mathbf{R}^*$ 关于乘法运算 · 所构成的代数结构$(\mathbf{R}^*, \cdot)$与实数集合 $\mathbf{R}$ 关于加法运算＋所构成的代数结构$(\mathbf{R}, +)$同构吗？为什么？

9. 设代数结构$(A, *)$和$(B,\circ)$中的运算都是 2 元的，在 $A\times B$ 上分别定义运算 Δ 如下：对于任意的$(x_1, y_1), (x_2, y_2)\in A\times B$，

$$(x_1, y_1)\Delta(x_2, y_2) = (x_1 * x_2, y_1 \circ y_2)$$

证明：$(A\times B, \Delta)$是代数结构，称为$(A, *)$和$(B,\circ)$中的**积代数**.

5.2 群的定义及性质

一元四次及以下的方程有求根公式. 在 1826 年由 24 岁挪威数学家 Niels Henrik Abel (1802—1829)证明了一般一元五次及以上方程 $a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0(a_0 \neq 0, n\geqslant 5)$不可能根式求解，完全解决了长达 200 多年的难题，并着手研究能用根式求解的方程的特征等问题，连当时的数学大师 Gauss 也未能理解其成果的重要意义，在贫困中渡过 27 个春秋的 Abel 因结核病死于 1829 年 4 月 6 日，三天后迟到的柏林大学数学教授聘书送达.

后来由法国数学家 Evarisfe Galois(1811—1832)继续 Abel 的工作，考虑哪些方程可以根式求解. 出身富裕、才思敏捷的 Galois 用根的置换构成的群等知识给出了能用根式求解方程的条件. 文章两次分别被 Cauchy 和 Fourier 遗失，而 Poisson“完全不能理解”，Galois 曾两次因政治罪入狱并于 1832 年 5 月 31 日决斗而死，死的前夜将结果寄给了他的朋友. 借助于 Galois 的研究工作，还可以证明自公元前 300 年 Euclid 开始长达 2000 年的限用圆规直尺的古希腊四大几何作图难题：将任意角三等分、作正 n 边形、倍立方(求作一个立方体使其体积为单位立方体体积的 2 倍)和化圆为方(求作正方形其面积为半径为 1 的圆的面积 π：π 是超越数)是不可能的. E. Galois 超越时代的天才思想在他去世约 40 年后才被人理解和接受，正是由于他的奇特思想和巧妙方法才有今天的近世代数，即代数结构.

群是研究相当成熟的一种代数结构，其研究方式是根据给定的几条规则去研讨其性质，推导过程是在符号之间进行的，因此是一种形式化方法，各种各样的逻辑演算系统也是采用这种方法. 这种形式化方法训练的重要性在计算机专业至关重要，因为计算机处理的就是符号. 同时群在组合计数、快速加法器设计、纠错码研制和椭圆曲线算法设计等方面有广泛而深入的应用.

本节对群这种代数结构进行较为详细的讨论，通过对它的讨论，可以洞察一般代数结构的讨论模式.

5.2.1 群的有关概念

群除有一个非空集合 G 外,更重要的是集合 G 上的代数运算“·”及所满足的运算性质.

【定义 5-10】 设 G 是非空集合,“·”是 G 上的 2 元代数运算,若下列 3 个条件成立,则 $(G,\cdot)$ 称为**群**(group).

(1) ·满足结合律：$\forall x,y,z\in G,(x\cdot y)\cdot z=x\cdot(y\cdot z)$.

(2) G 关于·有单位元,通常记为 e：$\forall x\in G, x\cdot e=e\cdot x=x$.

(3) G 中每一个元素在 G 中都有逆元：$\forall x\in G,\exists x^{-1}\in G, x\cdot x^{-1}=x^{-1}\cdot x=e$.

正如在第 1 章 1.3 节所说,运算符号可以根据需要选取,当然可以按上节用 * 号表示.选择“·”,是因为群中的运算可以读作“乘”(product 或 multiplication).同时,在仅讨论群时,可以省略运算符号,但我们不打算这样做.跟上节一样,在不强调群的运算符号时,可以将 $(G,\cdot)$ 记为 G.

容易验证,实数集合 $\mathbf{R}$ 关于数的加法运算+构成群 $(\mathbf{R},+)$.但 $\mathbf{R}$ 关于数的乘法运算·不能作成群,即 $(\mathbf{R},\cdot)$ 不是群,因为 $0\in\mathbf{R}$,但 0 关于乘法运算没有逆元,即不存在 $x\in\mathbf{R}$ 满足 $0\cdot x=x\cdot 0=1$.

【例 5-11】 验证：非 0 实数集合 $\mathbf{R}-\{0\}$ 关于数的乘法·运算构成群.

解 首先 $\mathbf{R}-\{0\}$ 关于·是封闭的：$\forall x,y\in\mathbf{R}-\{0\}$,有 $x\cdot y\in\mathbf{R}-\{0\}$.

$\mathbf{R}-\{0\}$ 上的数的乘法运算·满足

(1) 结合律：$\forall x,y,z\in\mathbf{R}-\{0\},(x\cdot y)\cdot z=x\cdot(y\cdot z)$.

(2) $\mathbf{R}-\{0\}$ 关于·有单位元 1：$\forall x\in\mathbf{R}-\{0\}, x\cdot 1=1\cdot x=x$.

(3) $\mathbf{R}-\{0\}$ 中每一个元素 $x\in\mathbf{R}-\{0\}$ 在 $\mathbf{R}-\{0\}$ 中都有逆元 $\frac{1}{x}=x^{-1}\in\mathbf{R}-\{0\}$：

$$x\cdot\frac{1}{x}=\frac{1}{x}\cdot x=1$$

因此,$(\mathbf{R}-\{0\},\cdot)$ 是群.

【例 5-12】 设 $G=\{e,a,b,c\}$,其上的“·”运算见表 5-5,容易验证 $(G,\cdot)$ 是群,称为 Klein 四元群.

表 5-5

·	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

【定义 5-11】 设 $(G,\cdot)$ 是群,若 $|G|=n<\infty$,则称 $(G,\cdot)$ 为 n 阶**有限群**(finite group);若 G 是无限集合,则 $(G,\cdot)$ 称为**无限群**(infinite group).

显然,上面两个例子所举的群都是无限群.下面是有限群的例子.

【例 5-13】 设 $A=\mathbf{R}-\{0,1\}$,在 A 上定义 6 个映射如下：对于任意 $x\in A$,

$$f_1(x)=x,\quad f_2(x)=\frac{1}{x},\quad f_3(x)=1-x,$$

$$f_4(x)=\frac{1}{1-x},\quad f_5(x)=\frac{x-1}{x},\quad f_6(x)=\frac{x}{x-1}$$

令 $G=\{f_1,f_2,f_3,f_4,f_5,f_6\}$，证明 G 关于映射(函数)的复合运算$\circ$构成群$(G,\circ)$.

证 首先证明 G 关于复合运算$\circ$是封闭的. 根据复合运算$\circ$的定义知

$$(f_i\circ f_j)(x)=f_j(f_i(x)),\quad i,j=1,2,3,4,5,6,$$

得到 G 关于复合运算$\circ$的运算表如表 5-6 所示.

表 5-6

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_6	f_5	f_1	f_2
f_5	f_5	f_6	f_2	f_1	f_4	f_3
f_6	f_6	f_5	f_4	f_3	f_2	f_1

例如，因为$(f_2\circ f_3)(x)=f_3(f_2(x))=f_3\left(\frac{1}{x}\right)=1-\frac{1}{x}=\frac{x-1}{x}=f_5(x)$，所以 $f_2\circ f_3=f_5$，其余类似.

由表 5-6 知，G 关于复合运算$\circ$是封闭的.

(1) 显然，复合运算$\circ$满足结合律.

(2) 由表 5-6 知，G 关于复合运算$\circ$的单位元是 f_1，因为 $f_1\circ f_i=f_i\circ f_1=f_i$，$i=1,2,3,4,5,6$.

(3) 由表 5-6 知 $f_5\circ f_4=f_4\circ f_5=f_1$，所以 $f_5^{-1}=f_4$ 且 $f_4^{-1}=f_5$. 类似地可得 $f_1^{-1}=f_1$，$f_2^{-1}=f_2$，$f_3^{-1}=f_3$，$f_6^{-1}=f_6$. 也就是说，G 中每个元素在 G 中都有逆元.

故$(G,\circ)$是群. 显然，$(G,\circ)$是 6 阶有限群.

【定义 5-12】 设$(G,\cdot)$是群，若其运算$\cdot$是可交换的，则称$(G,\cdot)$为**交换群**(commutative group)或**阿贝尔群**(Abel group).

容易知道，例 5-11 和例 5-12 是阿贝尔群，例 5-13 是非阿贝尔群.

设$(G,\cdot)$是群，e 是其单位元素，对于任意 $a\in G$，$n\in\mathbf{Z}$，

$$a^0=e;$$

$$a^n=\overbrace{a\cdot a\cdot\cdots\cdot a}^{n}\quad(n\text{ 为正整数});$$

$$a^n=\overbrace{a^{-1}\cdot a^{-1}\cdot\cdots\cdot a^{-1}}^{-n}\quad(n\text{ 为负整数}).$$

由定义知，对于负整数 n，有 $a^n=(a^{-1})^{-n}$.

元素 a 的阶是使得 $a^n=e$ 的最小正整数，用$|a|$表示.

与半群中只能定义元素的正整数方幂有所不同，因为 G 中有单位元素，可以定义 0 次方幂，因为每个元素都有逆元就可以定义负整数方幂.

需要注意的是，方幂运算是对群中的运算来说的. 如在群$(\mathbf{Z},+)$中，有 $3^{-1}=-3$，$3^2=$

$3+3=6, 3^{-2}=3^{-1}+3^{-1}=(-3)+(-3)=-6$ 等.

设$(G,\cdot)$是群,若存在$a\in G$,使得G中每个元素均为a的某整数方幂,则称$(G,\cdot)$为**循环群**(cycle group).

容易验证,$(\mathbf{Z}_m,+_m)$是m阶循环群,$(\mathbf{Z},+)$是无限循环群.

由群的定义知,群是含有幺元e的半群. 在下面讨论群的有关结论时,关键是利用"群中任意元素均存在逆元".

【定理 5-2】 设$(G,\cdot)$是群,则$\cdot$满足消去律.

证 对于任意$a,b,c\in G$,若$a\cdot b=a\cdot c$,因为$a\in G$有逆元$a^{-1}\in G$,于是有$a^{-1}\cdot(a\cdot b)=a^{-1}\cdot(a\cdot c)$,因此$(a^{-1}\cdot a)\cdot b=(a^{-1}\cdot a)\cdot c$,$e\cdot b=e\cdot c$,所以$b=c$. 这样,$\cdot$满足左消去律. 同理可证,$\cdot$满足右消去律.

5.2.2 子群

一般来说,子群比原来的群要"小",对子群的研究可以洞察原群的一些性质.

【定义 5-13】 设$(G,\cdot)$是群,$\varnothing\neq H\subseteq G$,若$H$关于群$G$的运算构成群,则称$(H,\cdot)$是$(G,\cdot)$的子群(subgroup),记为$(H,\cdot)\leqslant(G,\cdot)$,可简记为$H\leqslant G$.

根据定义容易验证$(Z,+)\leqslant(R,+)$.

对于任意群$(G,\cdot)$,设e为其单位元,则$\{e\}$和G都是G的子群,称为G的平凡子群.

【定理 5-3】 设$(G,\cdot)$是群,$\varnothing\neq H\subseteq G$,则$H\leqslant G$当且仅当下列条件成立:

(1) $\forall x,y\in H$,有$x\cdot y\in H$,且

(2) $\forall x\in H$,则x在G中的逆元$x^{-1}\in H$.

证 必要性显然. 为证明充分性,根据子群定义,只需证明G中的单位元$e\in H$即可.

因为H非空,必存在$a\in H$. 由(2)知,$a^{-1}\in H$. 由(1)知,$a\cdot a^{-1}=e\in H$.

【例 5-14】 设$(G,\cdot)$是群,令$Z(G)$表示所有与G中元素可交换的元素组成的集合,即$Z(G)=\{x\mid x\in G,\forall a\in G: x\cdot a=a\cdot x\}$,则$Z(G)\leqslant G$,称$Z(G)$为$G$的中心.

证 由于对于任意$a\in G$均有$e\cdot a=a\cdot e$,所以有$e\in Z(G)\neq\varnothing$.

(1) $\forall x,y\in Z(G)$,由已知对于任意$a\in G$有$x\cdot a=a\cdot x$,$y\cdot a=a\cdot y$,于是

$$(x\cdot y)\cdot a=x\cdot(y\cdot a)=x\cdot(a\cdot y)=(x\cdot a)\cdot y=(a\cdot x)\cdot y=a\cdot(x\cdot y),$$

所以有$x\cdot y\in Z(G)$.

(2) $\forall x\in Z(G)$,则对于任意$a\in G$有$a^{-1}\cdot x=x\cdot a^{-1}$,两边取逆得$x^{-1}\cdot a=a\cdot x^{-1}$,因此$x^{-1}\in Z(G)$.

由定理 5-3 知,$Z(G)\leqslant G$.

可以证明 **Lagrange 定理**:若G是有限群,$H\leqslant G$,则$|H|\,\big|\,|G|$.

群的同态与同构是借助于映射去讨论两个群之间的关系,它是研究群的一种重要方法.

5.2.3 群的同态

类似于 5.1 节一般代数结构间的同态映射定义如下。

【定义 5-14】 设$(G_1,*)$和$(G_2,\circ)$是群,如果存在$\varphi: G_1\to G_2$且φ保持运算,即对于任意$x_1,x_2\in G_1$,均有$\varphi(x_1*x_2)=\varphi(x_1)\circ\varphi(x_2)$,则称$\varphi$为群$(G_1,*)$到群$(G_2,\circ)$的同态映射,又称群$(G_1,*)$与群$(G_2,\circ)$同态. 若$\varphi$还是双射,则称$\varphi$为群$(G_1,*)$到群$(G_2,\circ)$的同构映射,又称群$(G_1,*)$与群$(G_2,\circ)$同构,记为$(G_1,*)\cong(G_2,\circ)$.

【例 5-15】 设$(\mathbf{R}^+, \cdot)$是正实数集合关于数的乘法运算构成的群,$(\mathbf{R}, +)$是实数集合关于数的加法运算构成的群,证明:群$(\mathbf{R}^+, \cdot)$与群$(\mathbf{R}, +)$同态.

证 令 $\varphi: \mathrm{R}^+ \to \mathrm{R}$, $\varphi(x)=\ln x$, $\forall x \in \mathrm{R}^+$. 对于任意 $x_1, x_2 \in \mathrm{R}^+$,因为

$$\varphi(x_1 \cdot x_2) = \ln(x_1 x_2) = \ln x_1 + \ln x_2 = \varphi(x_1) + \varphi(x_2),$$

所以,φ 是群$(\mathrm{R}^+, \cdot)$到群$(\mathrm{R}, +)$的同态映射. 故$(\mathrm{R}^+, \cdot)$与$(\mathrm{R}, +)$同态.

下例是不同构的两个群的例子.

【例 5-16】 证明:非 0 实数集合 $\mathbf{R}^*$ 关于乘法运算所构成的群$(\mathbf{R}^*, \cdot)$与实数集合 $\mathbf{R}$ 关于加法运算所构成的群$(\mathbf{R}, +)$不同构.

证 假设$(\mathbf{R}^*, \cdot) \cong (\mathbf{R}, +)$,则存在同构映射 φ,这时 $\varphi(1)=0$.

设 $\varphi(-1)=a$,则 $a \neq 0$,而 $\varphi(1)=\varphi((-1)\cdot(-1))=\varphi(-1)+\varphi(-1)=a+a=2a=0$,于是 $a=0$ 矛盾.

习 题 5.2

1. 令 $\mathbf{R}[x]$表示所有系数为实数的关于 x 的多项式组成的集合,验证 $\mathbf{R}[x]$关于多项式的加法运算构成群$(\mathbf{R}[x], +)$.

2. 令 $\boldsymbol{M}_n(\mathbf{R})$表示元素为实数的所有 n 阶方阵组成的集合,验证 $\boldsymbol{M}_n(\mathbf{R})$关于矩阵的加法运算构成群$(\boldsymbol{M}_n(\mathbf{R}), +)$,并说明 $\boldsymbol{M}_n(\mathbf{R})$关于矩阵的乘法运算 $\cdot$ 所作成的代数结构$(\boldsymbol{M}_n(\mathbf{R}), \cdot)$不能构成群.

3. 设 $\mathbf{Z}_m=\{0,1,2,\cdots,m-1\}$,$+_m$ 是模 m 加法运算,$\cdot_m$是模 m 乘法运算.

(1) 证明:$(\mathbf{Z}_m, +_m)$是群.

(2) 举例说明,一般情况下$(\mathbf{Z}_m-\{0\}, \cdot_m)$不是群,并推出$(\mathbf{Z}_m-\{0\}, \cdot_m)$是群的充要条件.

4. 设整数集合 $\mathbf{Z}$ 上定义 $*$ 运算如下:

$$\forall x, y \in \mathrm{Z}, x * y = x + y - 2.$$

证明:$(\mathbf{Z}, *)$是阿贝尔群.

5. 设 S 是任意非空集合,G 是所有 S 到 S 的所有双射组成的集合,则 G 关于映射的复合运算$\circ$构成群.

6. 设$(G, \cdot)$是群,若对于任意 $x \in G$ 都有 $x^2=e$,其中 e 为 G 中的单位元,则$(G, \cdot)$是阿贝尔群.

7. 集合 X 的幂集 $P(X)$关于集合的对称差运算$\oplus$构成群$(P(X), \oplus)$.

8. 证明:群$(G, \cdot)$只有单位元素是其唯一的幂等元素.

9. 设$(G, \cdot)$是有限群且$|G|$是偶数,则 G 中必存在元素 $x \neq e$ 满足 $x \cdot x=e$,其中 e 为 G 中的单位元.

10. 设$(G, \cdot)$是有限半群,若 $\cdot$ 运算满足消去律,则$(G, \cdot)$是群.

11. 设 $G=\{f \mid f: \mathbf{R} \to \mathbf{R}, \exists a, b \in \mathbf{R}, a \neq 0, f(x)=ax+b\}$,$G$ 上的运算为映射的复合$\circ$,则

(1) $(G, \circ)$是群.

(2) 设 $H=\{f \mid f \in G, f(x)=x+b\}$,则 $H \leqslant G$.

(3) 设 $K=\{f \mid f \in G, f(x)=ax\}$,则 $K \leqslant G$.

12. 设 $G=\{(x,y)\mid x,y\in\mathbf{R},x\neq 0\}$,对于任意$(x_1,y_1)\in G$ 和$(x_2,y_2)\in G$ 定义

$$(x_1,y_1)\cdot(x_2,y_2)=(x_1x_2,x_2y_1+y_2),$$

证明

(1) $(G,\cdot)$是非阿贝尔群.

(2) 令 $H=\{(1,y)\mid y\in\mathrm{R}\}$,则 $H\leqslant G$.

13. 令 φ: $\mathbf{R}\to\mathbf{R}^*$, $\varphi(x)=\mathrm{e}^x$,证明:φ 是$(\mathbf{R},+)$到$(\mathbf{R}^*,\cdot)$的同态映射.

5.3 环 和 域

群是仅有一个二元运算的代数结构,环是有两个二元运算的代数结构.环理论在计算机科学特别是在编码理论的研究中有诸多应用.

5.3.1 环的定义

【定义 5-15】 设$(R,+,\cdot)$是含两个二元运算的代数结构,若

(1) $(R,+)$是阿贝尔群.

(2) $(R,\cdot)$是半群.

(3) $\cdot$ 对$+$可分配.

则称$(R,+,\cdot)$是**环**(ring).

为了方便,通常将环的第一种运算$+$称为加法,第二种运算$\cdot$称为乘法,同时规定乘法运算较加法运算级别高.跟以前一样,环的加法和乘法一般不是数的加法和乘法.

下面是几种常见的环的例子.

【例 5-17】 容易验证关于数的加法和乘法运算,下列代数结构是环.

(1) $(\mathbf{Z},+,\cdot)$(整数环).

(2) $(\mathbf{R},+,\cdot)$.

【例 5-18】 设 R 是所有 n 阶整数矩阵组成的集合,则 R 对于矩阵的加法运算$+$和矩阵的乘法运算$\cdot$构成环,称为**矩阵环**.

解 (1) $(R,+)$是阿贝尔群,其加法幺元为零矩阵 0,任意元素 $\boldsymbol{A}\in R$ 关于加法的逆元为其负矩阵$-\boldsymbol{A}$.

(2) $(R,\cdot)$是半群.

(3) 矩阵乘法运算 $\cdot$ 对加法运算$+$可分配,即对于任意 $\boldsymbol{A},\boldsymbol{B},\boldsymbol{C}\in R$ 有

$$\boldsymbol{A}\cdot(\boldsymbol{B}+\boldsymbol{C})=\boldsymbol{A}\cdot\boldsymbol{B}+\boldsymbol{A}\cdot\boldsymbol{C}$$

$$(\boldsymbol{B}+\boldsymbol{C})\cdot\boldsymbol{A}=\boldsymbol{B}\cdot\boldsymbol{A}+\boldsymbol{C}\cdot\boldsymbol{A}$$

因此$(R,+,\cdot)$是环.

【例 5-19】 验证,$\mathbf{Z}_n=\{0,1,2,\cdots,n-1\}$对于模 n 加法运算$+_n$ 和模 n 乘法运算 $\cdot_n$构成环,称为**模 n 剩余类环**.

【例 5-20】 设所有实数集合 $\mathbf{R}$ 上的关于 x 的多项式组成的集合为 $\mathbf{R}[x]$,则 $\mathbf{R}[x]$对于多项式的加法运算$+$和多项式的乘法运算$\cdot$构成环,称为 $\mathbf{R}$ 上的**多项式环**.

5.3.2 几种特殊的环

下面介绍几种特殊的环.

【定义 5-16】 设$(R, +, \cdot)$是环,若

(1) R 中的乘法运算 $\cdot$ 可交换,则称$(R,+,\cdot)$是**交换环**.

(2) R 中的乘法运算 $\cdot$ 有幺元,则称$(R,+,\cdot)$是**含幺环**,其乘法幺元记为 1.

(3) 对于任意 $x\neq 0, y\neq 0$ 均有 $x\cdot y\neq 0$,则称$(R,+,\cdot)$是**无零因子环**,其中 0 是环的零元(加法幺元).

(4) $(R, +, \cdot)$是含幺、无零因子、交换环,则称$(R, +, \cdot)$为**整环**(integral domain).

(5) $(R, +, \cdot)$是含幺环且任意 $a(a\neq 0$ 且 $a\in R)$关于乘法运算都有逆元,则称$(R, +, \cdot)$为**除环**.

关于交换环或含幺环的判断是容易的,对于无零因子环有以下说明.

① 环的零元是加法幺元.

② 对于整数环$(\mathbf{Z}, +, \cdot)$,因为其零元是 0,对于任意 $x\neq 0, y\neq 0$ 均有 $x\cdot y\neq 0$,所以整数环$(\mathbf{Z}, +, \cdot)$是无零因子环.

③ 若 $x\neq 0, y\neq 0$ 且 $x\cdot y=0$,则称 x 和 y 是零(的)因子. 含有零因子的环称为**有零因子环**. 例如,对于模 6 剩余类环$(\mathbf{Z}_6, +_6, \cdot_6)$,其零元为 0,显然 $2\neq 0, 3\neq 0$,但$2\cdot_6 3=0$,所以 2 和 3 是零因子,因此环$(\mathbf{Z}_6, +_6, \cdot_6)$是有零因子环.

【例 5-21】 对于 $m>1$,模 m 剩余类环$(\mathbf{Z}_m, +_m, \cdot_m)$是无零因子环的充要条件是 m 为素数.

证 ($\Rightarrow$)假设 m 不是素数,则存在正整数 $k, l\in\mathbf{Z}_m$ 使得 $kl=m$,这时 $k\neq 0, l\neq 0$,而 $k\cdot_m l=0$,所以 $k, l\in\mathbf{Z}_m$ 是零因子,与$(\mathbf{Z}_m, +_m, \cdot_m)$是无零因子环矛盾.

($\Leftarrow$)若 m 为素数,对于任意 $k, l\in\mathbf{Z}_m$,若 $k\neq 0, l\neq 0$,则 $kl(\mathrm{mod}\, m)\neq 0$,于是 $k\cdot_n l\neq 0$,因此$(\mathbf{Z}_m, +_m, \cdot_m)$是无零因子环.

根据定义,在 $m=1$ 时,$(\{0\}, +, \cdot)$也是无零因子环.

很容易验证,$(\mathbf{Z}, +, \cdot)$是整环但不是除环. 下面介绍一个重要的除环的例子——**四元数除环**,在计算机图形学中,**四元数**(quaternion)可用于讨论四维分形的三维投影.

【例 5-22】 设 i, j, k 是 3 个符号,规定 i, j, k 之间的乘法如表 5-7 所示. 称 $a+b\mathrm{i}+c\mathrm{j}+d\mathrm{k}$ 为四元数,其中 a, b, c, d 是实数. 所有四元数组成的集合为 R,对于任意 $a_1+b_1\mathrm{i}+c_1\mathrm{j}+d_1\mathrm{k}\in R$ 和 $a_2+b_2\mathrm{i}+c_2\mathrm{j}+d_2\mathrm{k}\in R$,规定其上的加法运算+为"合并同类项":

$$(a_1+b_1\mathrm{i}+c_1\mathrm{j}+d_1\mathrm{k})+(a_2+b_2\mathrm{i}+c_2\mathrm{j}+d_2\mathrm{k})$$
$$=(a_1+a_2)+(b_1+b_2)\mathrm{i}+(c_1+c_2)\mathrm{j}+(d_1+d_2)\mathrm{k}$$

表 5-7

·	i	j	k
i	−1	k	−j
j	−k	−1	i
k	j	−i	−1

其上的乘法运算 $\cdot$ 为"使用分配律展开,按表 5-7 的乘法计算,再合并同类项":

$$(a_1+b_1\mathrm{i}+c_1\mathrm{j}+d_1\mathrm{k})\cdot(a_2+b_2\mathrm{i}+c_2\mathrm{j}+d_2\mathrm{k})$$
$$=(a_1a_2-b_1b_2-c_1c_2-d_1d_2)+(a_1b_2+a_2b_1+c_1d_2-d_1c_2)\mathrm{i}+$$
$$(a_1c_2+a_2c_1+b_2d_1-b_1d_2)\mathrm{j}+(a_1d_2+a_2d_1+b_1c_2-b_2c_1)\mathrm{k}$$

则$(R, +, \cdot)$是除环.

证 容易验证$(R, +, \cdot)$是环. 对于任意 $0\neq a+b\mathrm{i}+c\mathrm{j}+d\mathrm{k}\in R$,其乘法逆元为

$$(a+b\mathrm{i}+c\mathrm{j}+d\mathrm{k})^{-1}=\frac{1}{a^2+b^2+c^2+d^2}(a-b\mathrm{i}-c\mathrm{j}-d\mathrm{k})$$

所以$(R, +, \cdot)$是除环. 但注意到,R 关于乘法运算 $\cdot$ 不可交换.

5.3.3 域的定义

【定义 5-17】 设$(F,+,\cdot)$是环,若$(F-\{0\},\cdot)$是阿贝尔群,则称$(F,+,\cdot)$是**域**(field).

根据定义知道,对于域$(F,+,\cdot)$有$|F|\geqslant 2$.

【例 5-23】 验证:$(\mathbf{R},+,\cdot)$是域,而整数环$(\mathbf{Z},+,\cdot)$不是域.

解 因为$(\mathbf{R},+,\cdot)$是环且$(\mathbf{R}-\{0\},\cdot)$是阿贝尔群,所以$(\mathbf{R},+,\cdot)$是域.

虽然$(\mathbf{Z},+,\cdot)$是环,但$(\mathbf{Z}-\{0\},+,\cdot)$不是群,因为 $\mathbf{Z}$ 中除 1 和 -1 外其余元素关于乘法运算在 $\mathbf{Z}$ 中都没有逆元.

实际上,常见的 3 种数域分别为有理数域$(\mathbf{Q}, +, \cdot)$、实数域$(\mathbf{R}, +, \cdot)$、复数域$(\mathbf{C}, +, \cdot)$.

【例 5-24】 设 $F=\{a+b\sqrt{3}\mid a,b\in\mathbf{Q}\}$,则 F 关于数的加法$+$和矩阵乘法 $\cdot$ 构成域.

证 容易验证$(F,+,\cdot)$是环. 对于任意 $0\neq a+b\sqrt{3}\in F$,若 $a-b\sqrt{3}\neq 0$,则 $1/(a+b\sqrt{3})=a/(a^2-3b^2)-b\sqrt{3}/(a^2-3b^2)\in F$,若 $a-b\sqrt{3}=0$,则 $a=b\sqrt{3}\neq 0$,这时 $1/(a+b\sqrt{3})=\sqrt{3}/6b\in F$. 于是 $a+b\sqrt{3}\neq 0$ 均有逆元,因此$(F-\{0\},\cdot)$是阿贝尔群,进而$(F,+,\cdot)$是域.

由于$(\mathbf{R}, +, \cdot)$是整环,由例 5-23 可进一步证明下例.

【例 5-25】 证明:域是整环,但整环不一定是域.

证 对于域$(F,+,\cdot)$,显然它是含幺交换环. 对于任意 $0\neq x,y\in F$,若 $x\cdot y=0$,因为 x^{-1}存在,于是 $x^{-1}\cdot(x\cdot y)=x^{-1}\cdot 0$,因此 $y=0$,与 $y\neq 0$ 矛盾,因此$(F,+,\cdot)$是无零因子环. 所以域$(F,+,\cdot)$是整环.

显然$(\mathbf{Z},+,\cdot)$是整环但不是域.

下面证明:

【定理 5-4】 阶$\geqslant 2$ 的有限整环是域.

证 设$(F,+,\cdot)$是有限整环,只需证明$(F-\{0\},\cdot)$是群即可. 对于任意 $a\in F-\{0\}$,令 $aF=\{a\cdot x\mid x\in F\}$,构造映射

$$f: F\rightarrow aF, f(x)=a\cdot x, \forall x\in F$$

(1) 若 $f(x_1)=f(x_2)$,即 $a\cdot x_1=a\cdot x_2$,由于 $a\neq 0$,于是 $x_1=x_2$,所以 f 是单射.

(2) 对于任意 $y\in aF$,存在 $x\in F$ 使得 $y=a\cdot x$,于是 $f(x)=y$,即 f 是满射.

因为 F 有限且 $aF\subseteq F$,所以 $F=aF$. 由于 $1\in F=aF$,必存在 $b\in F$ 使得 $a\cdot b=1$,于是 b 是 a 关于乘法运算的逆元.

故$(F,+,\cdot)$是域.

5.3.4 有限域

有限域(finite field)称为 Galois 域,有 q 个元素的 Galois 域记为 $\mathrm{GF}(q)$.

有限域理论在计算机密码学中有着非常重要的应用，特别是研究公钥密码学中的大素数测试算法和椭圆曲线密码体制(elliptic curve cryptography).

【例 5-26】 验证：环$(\mathbf{Z}_5, +_5, \cdot_5)$是域，但$(\mathbf{Z}_6, +_6, \cdot_6)$不是域.

解 因为$(\mathbf{Z}_5, +_5, \cdot_5)$是交换环，只需验证$(\mathbf{Z}_5-\{0\}, \cdot_5)$是群即可. 由于$1\cdot_5 1=1$, $2\cdot_5 3=1$, $4\cdot_5 4=1$，于是对于乘法运算来说有$1^{-1}=1$, $2^{-1}=3$, $3^{-1}=2$, $4^{-1}=4$.

对于环$(\mathbf{Z}_6, +_6, \cdot_6)$，因为$2\cdot_6 3=0$，2 和 3 是零因子，所以$(\mathbf{Z}_6, +_6, \cdot_6)$不是整环，进而不是域.

可以证明：

【定理 5-5】 环$(\mathbf{Z}_m, +_m, \cdot_m)$是域当且仅当 m 是素数.

证 ($\Rightarrow$) 若 m 不是素数，即存在$1<k, l<m$使得$m=kl$，这时$0\neq k, l\in\mathbf{Z}_m$且$k\cdot_m l=0$，$k$ 和 l 是零因子，与已知$(\mathbf{Z}_m, +_m, \cdot_m)$是域矛盾.

($\Leftarrow$)设 m 是素数，对于任意$0\neq x\in\mathbf{Z}_m$，则 x 与 m 互素，即存在整数 p, q 使得$px+qm=1$，这时$(px+qm)(\bmod m)=1$，于是$p(\bmod m)\cdot_m x=1$，因此 x 的关于乘法运算的逆元为$p(\bmod m)\in\mathbf{Z}_m$.

下面将不加证明地给出几个关于有限域的结论，先给出域的同态与同构的定义.

【定义 5-18】 设$(F_1, +, \cdot)$和$(F_2, \oplus, \odot)$是域，若 φ: $F_1\to F_2$ 且 φ 分别保持域的加法运算和乘法运算，即

$$\varphi(x_1+x_2)=\varphi(x_1)\oplus\varphi(x_2)$$
$$\varphi(x_1\cdot x_2)=\varphi(x_1)\odot\varphi(x_2)$$

则称 φ 为$(F_1, +, \cdot)$到$(F_2, \oplus, \odot)$的**域同态映射**. 若 φ 是双射且 φ 是域同态映射，则称 φ 为$(F_1, +, \cdot)$到$(F_2, \oplus, \odot)$的**域同构映射**，又称域$(F_1, +, \cdot)$与$(F_2, \oplus, \odot)$**同构**，记为$(F_1, +, \cdot)\cong(F_2, \oplus, \odot)$.

【定理 5-6】 下面结论成立：

(1) 设$(F, +, \cdot)$是有限域，则存在素数 p 和正整数 n 使得$|F|=p^n$.

(2) 对于任意素数 p 和正整数 n，存在 p^n 个元素的有限域.

(3) 元素个数相同的有限域是同构的.

习 题 5.3

1. 验证整数集合 $\mathbf{Z}$ 关于数的加法$+$和乘法运算$\cdot$构成环.

2. 设$R=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d\in\mathbf{Z}\right\}$，则 R 关于矩阵的加法$+$和矩阵乘法$\cdot$构成环.

3. 设$R=\{a+b\sqrt{3} \mid a, b\in\mathbf{Z}\}$，则 R 关于数的加法$+$和矩阵乘法$\cdot$构成环.

4. 设 R 是区间$(-\infty, +\infty)$上的所有连续函数组成的集合，对于任意 $f, g\in R$，定义

$$(f+g)(x)=f(x)+g(x), (f\circ g)(x)=f(g(x)), \forall x\in(-\infty, +\infty)$$

试判断$(R, +, \circ)$是否能构成环.

5. 设 X 是集合，$P(X)$是 X 的幂集，证明：$P(X)$关于集合的对称差运算$\oplus$和集合的交运算$\cap$构成环$(P(X), \oplus, \cap)$.

6. 证明：$(\mathbf{R}[x], +, \cdot)$是整环但不是除环.

7. 证明：乘法运算可交换的除环是整环.

8. 设 $R=\{a+b\mathrm{i}|a,b\in\mathbf{Q}\}$，则 R 关于数的加法＋和矩阵乘法 · 构成除环，该环称为**高斯数环**.

9. 设 $R=\mathbf{Z}\times\mathbf{Z}$，定义 R 上的加法＋运算和乘法 · 运算如下：
对于任意 $(x_1,y_1)\in R,(x_2,y_2)\in R$，

$$(x_1,y_1)+(x_2,y_2)=(x_1+x_2,y_1+y_2)$$
$$(x_1,y_1)\cdot(x_2,y_2)=(x_1\cdot x_2,y_1\cdot y_2)$$

证明：$(R,+,\cdot)$是环，并求出该环的所有零因子.

10. 设$(R,+,\cdot)$是含幺交换环，$x\notin R$ 是未定元，对于任意 $r\in R,x\cdot r=r\cdot x$. 令 $R[x]=\{f(x)|f(x)=a_0+a_1x+\cdots+a_nx^n,a_i\in R,i=0,1,\cdots,n-1,n\in\mathbf{N}\}$，则 $R[x]$关于多项式的加法＋和乘法 · 构成环，称$(R[x],+,\cdot)$为**环 R 上的关于 x 的一元多项式环**.

11. 设$(R,+,\cdot)$是环，若 R 的乘法运算 · 满足幂等性，即对于任意 $x\in R$ 有 $x\cdot x=x$，则称$(R,+,\cdot)$是**布尔环**. 证明：

(1) 对于任意 $x\in R$ 有 $x+x=0$.

(2) 布尔环是交换环.

(3) 若$|R|>2$，则$(R,+,\cdot)$不是整环.

12. 设$(R,+,\cdot)$是环，$A=R^R$，定义 A 上的运算分别为函数的加法与乘法，即：对于任意 $f,g\in A,(f+g)(x)=f(x)+g(x),(f\cdot g)(x)=f(x)\cdot g(x),\forall x\in R$. 证明：$(A,+,\cdot)$是环.

13. 设$(R,+,\cdot)$是含幺 1 的环，对于任意 $x,y\in R$，定义

$$x\oplus y=x+y+1,\quad x\odot y=x\cdot y+x+y$$

证明：

(1) $(R,\oplus,\odot)$是含幺环.

(2) 令 $\varphi(x)=x-1$，则 φ 是环$(R,+,\cdot)$到环$(R,\oplus,\odot)$的同构映射.

14. 验证：高斯数环$(R,+,\cdot)$是域，其中 $R=\{a+b\mathrm{i}|a,b\in\mathbf{Q}\}$.

15. 构造一个 3 阶域$(F,+,\cdot)$的运算表.

16. 设$(\mathbf{C},+,\cdot)$是复数域，令 φ：$\mathbf{C}\to\mathbf{C},\varphi(a+b\mathrm{i})=a-b\mathrm{i}$，其中 $\mathrm{i}^2=-1$，则 φ 是$(\mathbf{C},+,\cdot)$的自同构映射.

5.4 格与布尔代数

格论是 Dedekind 在 1935 年研究交换环及其理想时提出的，它是一种重要的代数结构. 格论是计算机语言的指称语义的理论基础，在计算机应用逻辑研究中有着重要作用.

布尔代数是英国数学家 George Boole 在 1847 年左右在对逻辑思维法则进行研究时提出的，后来很多数学家特别是 E. V. Hungtington 和E. H. Stone对布尔代数进行了一般化研究，在 1938 年 C. E. Shannon 发表的 A Symbolic Analysis of Relay and Switching Circuits 论文，为布尔代数在工艺技术中的应用开创了先河，自此以后布尔代数在自动推理和逻辑电路设计的分析和优化等问题的讨论中都有着最直接的应用，作为计算机设计基础的《数字逻辑》就是布尔代数.

本节先介绍格，在此基础上引入分配格和有补格，而把布尔代数作为一种特殊的格加以讨论. 格和布尔代数都是按“序结构”进行的讨论，它们本质上也是代数结构.

5.4.1 格的定义和性质

设$(L,\leqslant)$是偏序集，$\leqslant$是L上的偏序. 一般来说L中的两个元素的上确界及下确界不一定存在. 例如哈斯图如图5-1所示的偏序集，$\{c,b\}$无上确界，$\{a,d\}$无下确界.

【定义 5-19】 设$(L,\leqslant)$是偏序集，若L中任意两个元素都存在上确界以及下确界，则称$(L,\leqslant)$是**格**(lattice). 为了方便，这样的格可称为**偏序格**.

根据定义知，如图5-2和图5-3所示的偏序集都是格.

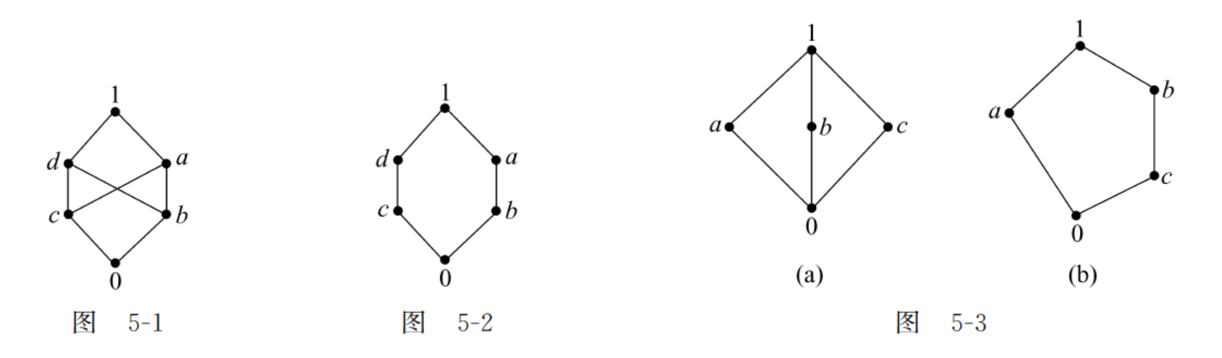


图 5-1　　图 5-2　　图 5-3

如图5-3(a)所示称为**钻石格**，如图5-3(b)所示称为**五角格**.

【例 5-27】 证明：$(P(X),\subseteq)$是格，其中$P(X)$是集合X的幂集.

证 显然，$(P(X),\subseteq)$是偏序集. 对于任意$A,B\in P(X)$，就集合包含关系来说，有$\sup\{A,B\}=A\cup B\in P(X)$，$\inf\{A,B\}=A\cap B\in P(X)$，所以$(P(X),\subseteq)$是格.

如图5-4(a)～图5-4(c)所示分别是$X=\{a\},\{a,b\},\{a,b,c\}$时格$(P(X),\subseteq)$的哈斯图.

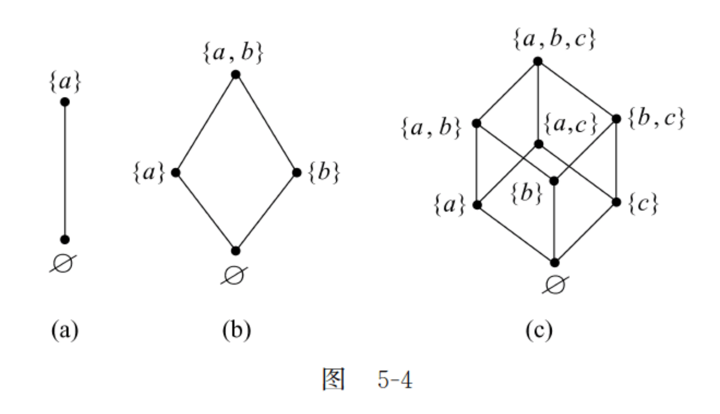


图 5-4

类似地，所有A到B的关系构成的集合$\mathscr{R}$关于包含关系“$\subseteq$”构成格$(\mathscr{R},\subseteq)$.

【例 5-28】 证明：$(D_n,|)$是格，其中D_n是自然数n的正因数组成的集合，$|$是其上的整除关系.

证 显然，$(D_n,|)$是偏序集. 根据整除关系定义知，对于任意$x,y\in D_n$有

$\sup\{x,y\}=\mathrm{LCM}(x,y)=[x,y]\in D_n$；$\inf\{x,y\}=\mathrm{GCD}(x,y)=(x,y)\in D_n$. 所以，$(D_n,|)$是格.

如图5-5所示分别是$n=8,6,30$时格$(D_n,|)$的哈斯图.

【例 5-29】 令F是所有合式公式(WFF)组成的集合，$\Rightarrow$是公式间的逻辑蕴涵关系，则

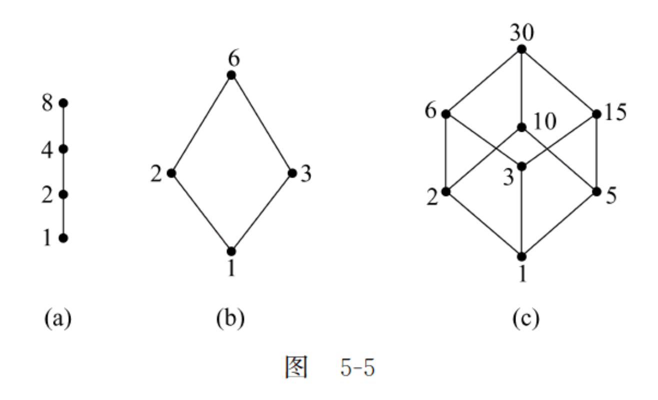


图 5-5

$(F,\Rightarrow)$是格.

证 显然,$(F,\Rightarrow)$是偏序集.就逻辑蕴涵关系$\Rightarrow$来说,对于任意$A,B\in F$.

(1) 由于$A\Rightarrow A\vee B$,$B\Rightarrow A\vee B$,于是$A\vee B$是$\{A,B\}$的上界.如果$A\Rightarrow C$,$B\Rightarrow C$,那么$A\vee B\Rightarrow C$,所以$\sup\{A,B\}=A\vee B\in F$.

(2) 因为$A\wedge B\Rightarrow A$,$A\wedge B\Rightarrow B$,于是$A\wedge B$是$\{A,B\}$的下界.如果$C\Rightarrow A$,$C\Rightarrow B$,那么$C\Rightarrow A\wedge B$,所以$\inf\{A,B\}=A\wedge B\in F$.

由(1)和(2)知,$(F,\Rightarrow)$是格.

设$(L,\leqslant)$是格,对于任意$x,y\in L$,$\{x,y\}$的上确界$\sup\{x,y\}\in L$存在且$\{x,y\}$的下确界$\inf\{x,y\}\in L$存在,这时$\sup\{x,y\}$和$\inf\{x,y\}$还是唯一的,因此可以定义格上的求上确界运算“+”和求下确界运算“·”.

【定义 5-20】 设$(L,\leqslant)$是格,对于任意$x,y\in L$,分别定义格上的**求上确界运算**“+”和**求下确界运算**“·”为

$$x+y=\sup\{x,y\} \tag{1}$$

$$x\cdot y=\inf\{x,y\} \tag{2}$$

例如,在格$(P(X),\subseteq)$中,对于任意$A,B\in P(X)$有

$$A+B=A\cup B,\quad A\cdot B=A\cap B$$

在例 6-3 中的格$(F,\Rightarrow)$中,对于任意$A,B\in F$有

$$A+B=A\vee B,\quad A\cdot B=A\wedge B$$

显然,格$(L,\leqslant)$上求上确界运算“+”和求下确界运算“·”是L上的代数运算.

格中的“+”是求上确界运算,可以看作是格的加法运算,读作“加”;同样,格中的“·”是求下确界运算,可以看作是格的乘法运算,读作“乘”.

这种表示格的求上(下)确界运算的符号+(·)与通常所采用的运算符号$\vee$($\wedge$)不尽一致,这样做是为了与后面讨论的布尔代数所采用的运算符号一致.通过第 5 章的学习,所用符号不会引起任何混淆,且便于读写.

由于“上确界$\leqslant$上界”以及“下界$\leqslant$下确界”,根据定义 5-20 易知.

【定理 5-7】 设$(L,\leqslant)$是格,则对于任意$x,y\in L$有:

(1) $x\leqslant x+y$,$y\leqslant x+y$;

(2) $x\cdot y\leqslant x$,$x\cdot y\leqslant y$.

为了方便讨论格的其他性质,先介绍格的对偶原理,它本身是格的重要性质之一.

设$(L,\leqslant)$是格,$\geqslant$ 是$\leqslant$ 的逆关系,即 $y\geqslant x\Leftrightarrow x\leqslant y$.显然,$(L,\geqslant)$是格.$(L,\leqslant)$与

$(L,\geqslant)$的哈斯图是互为颠倒的.于是,对于任意 $x,y\in L$ 有

$$\sup_{(L,\leqslant)}\{x,y\}=\inf_{(L,\geqslant)}\{x,y\},\quad \inf_{(L,\leqslant)}\{x,y\}=\sup_{(L,\geqslant)}\{x,y\}$$

若 L 关于$\leqslant$存在最大元素,记为 1,则$(L,\geqslant)$有最小元素,记为 0;若 L 关于$\leqslant$存在最小元素 0,则$(L,\geqslant)$有最大元素 1.

【定义 5-21】 对于任意关于格$(L,\leqslant)$的命题,将命题前提和结论中的 (1)$\leqslant$改为$\geqslant$;(2)$+$ 改为$\cdot$;(3) $\cdot$ 改为$+$;(4)0 改为 1;(5)1 改为 0 所得到的命题称为原命题的**对偶命题**.

显然有下列定理:

【定理 5-8】 对于任意关于格$(L,\leqslant)$的真命题,其对偶命题亦为真.

例如,在定理 5-7 中,由 $x\leqslant x+y$ 可得出 $x\geqslant x\cdot y$,即 $x\cdot y\leqslant x$.由 $y\leqslant x+y$ 可得出 $y\geqslant x\cdot y$,即 $x\cdot y\leqslant y$.

在格的性质中,有很多都是成对出现的.在下面定理的证明中,注意“上确界$\leqslant$上界”以及“下界$\leqslant$下确界”技巧的充分利用.

【定理 5-9】 设$(L,\leqslant)$是格,对于任意 $x_1,x_2,y_1,y_2\in L$,若 $x_1\leqslant y_1$ 且 $x_2\leqslant y_2$,则 $x_1+x_2\leqslant y_1+y_2$ 且 $x_1\cdot x_2\leqslant y_1\cdot y_2$.

证 根据定理 5-7 有 $y_1\leqslant y_1+y_2$ 及 $y_2\leqslant y_1+y_2$,由已知条件 $x_1\leqslant y_1$ 且 $x_2\leqslant y_2$ 以及符号$\leqslant$的传递性知

$$x_1\leqslant y_1+y_2 \quad 且 \quad x_2\leqslant y_1+y_2$$

于是 y_1+y_2 是$\{x_1,x_2\}$的上界,而 x_1+x_2 是$\{x_1,x_2\}$的上确界,根据“上确界$\leqslant$上界”知 $x_1+x_2\leqslant y_1+y_2$.

同理可证 $x_1\cdot x_2\leqslant y_1\cdot y_2$.

事实上,“若 $x_1\leqslant y_1$ 且 $x_2\leqslant y_2$,则 $x_1+x_2\leqslant y_1+y_2$”的对偶命题是“若 $x_1\geqslant y_1$ 且 $x_2\geqslant y_2$,则 $x_1\cdot x_2\geqslant y_1\cdot y_2$”,即“若 $x_1\leqslant y_1$ 且 $x_2\leqslant y_2$,则 $x_1\cdot x_2\leqslant y_1\cdot y_2$”.

定理 5-9 所述性质称为格的**保序性**.在格$(L,\leqslant)$中,对于任意 $x\in L$,由于$x+x=\sup\{x,x\}=x$ 及 $x\cdot x=\inf\{x,x\}=x$,所以格的加法运算$+$以及格的乘法运算$\cdot$具有幂等性.

设$(L,\leqslant)$是格,对于任意 $x\in L$ 有 $x+x=x$ 及 $x\cdot x=x$.

下面的定理 6-5 是格的**特征性质**.

【定理 5-10】 设$(L,\leqslant)$是格,对于任意 $x,y,z\in L$ 有:

(1) **交换性** $x+y=y+x$,$x\cdot y=y\cdot x$;

(2) **结合性** $(x+y)+z=x+(y+z)$,$(x\cdot y)\cdot z=x\cdot(y\cdot z)$;

(3) **吸收性** $x+(x\cdot y)=x$,$x\cdot(x+y)=x$.

证 (1) 显然.

(2) 由于 $x\leqslant x+(y+z)$,$y\leqslant y+z\leqslant x+(y+z)$,于是 $x+y\leqslant x+(y+z)$.又因为 $z\leqslant y+z\leqslant x+(y+z)$,因此$(x+y)+z\leqslant x+(y+z)$.

同样可得 $x+(y+z)\leqslant(x+y)+z$.所以$(x+y)+z=x+(y+z)$.

利用对偶原理有$(x\cdot y)\cdot z=x\cdot(y\cdot z)$.

(3) 因为 $x\leqslant x$ 且 $x\cdot y\leqslant x$,所以 $x+(x\cdot y)\leqslant x$.而显然 $x\leqslant x+(x\cdot y)$,因此 $x+(x\cdot y)=x$.

利用对偶原理有 $x\cdot(x+y)=x$.

正因为如此,将具有两个2元运算且满足上述定理(1)、(2)和(3)的代数结构$(L,+,\cdot)$称为格,这样定义的格称为**代数格**. 可以证明偏序格和代数格本质相同.

在序结构的讨论中,保序映射是序结构中的重要概念.

【定义 5-22】 设$(L_1,\leqslant_1)$和$(L_2,\leqslant_2)$是格,存在 φ: $L_1\to L_2$,对于任意 $x_1,x_2\in L_1$,若 $x_1\leqslant_1 x_2$,有 $\varphi(x_1)\leqslant_2\varphi(x_2)$,则称 φ 为格$(L_1,\leqslant_1)$到格$(L_2,\leqslant_2)$的**保序映射**.

保序映射可以进一步推广到一般的关系 R 上考虑.

【例 5-30】 设$(S,\leqslant)$是格,其哈斯图如图5-3(b)所示. 令 φ: $S\to P(S)$,

$$\varphi(x)=\{y\mid y\in L, y\leqslant x\}$$

则 φ 是格$(S,\leqslant)$到格$(P(S),\subseteq)$的保序映射.

证 根据 φ 的定义有 $\varphi(1)=S$,$\varphi(a)=\{0,a\}$,$\varphi(b)=\{0,b,c\}$,$\varphi(c)=\{0,c\}$,$\varphi(0)=\{0\}$. 显然,当 $x_1\leqslant x_2$,有 $\varphi(x_1)\subseteq\varphi(x_2)$,所以 φ 为格$(S,\leqslant)$到格$(P(S),\subseteq)$的保序映射.

5.4.2 分配格

有例子表明,格不满足分配性.

【例 5-31】 举例说明在格$(L,\leqslant)$中,格的乘法运算"·"和格加法运算"+"相互不一定可分配.

解 在图5-3(a)中,因为 $a\cdot(b+c)=a\cdot 1=a$,而$(a\cdot b)+(a\cdot c)=0+0=0$,所以 $a\cdot(b+c)\neq(a\cdot b)+(a\cdot c)$,即格的乘法运算"·"对格的加法运算"+"不可分配.

同样,由于 $a+(b\cdot c)=a+0=a$,而$(a+b)\cdot(a+c)=1\cdot 1=1$,所以 $a+(b\cdot c)\neq(a+b)\cdot(a+c)$,即格的加法运算"+"对格的乘法运算"·"不可分配.

【定义 5-23】 设$(L,\leqslant)$是格,若格的乘法运算"·"对格的加法运算"+"可分配(或格的加法运算"+"对格的乘法运算"·"可分配),则称$(L,\leqslant)$为**分配格**(distributive lattice).

【例 5-32】 证明:$(P(X),\subseteq)$是分配格.

证 由于格$(P(X),\subseteq)$诱导的代数结构为$(P(X),\cup,\cap)$,对于任意 $A,B,C\in P(X)$,显然有

$$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$$

所以$(P(X),\subseteq)$是分配格.

事实上,$(F,\Rightarrow)$也是分配格,其中 F 是所有合式公式组成的集合,$\Rightarrow$是公式间的逻辑蕴涵关系.

由例5-30知,钻石格不是分配格. 实际上,五角格也不是分配格. 钻石格和五角格是两个非常重要的非分配格的例子. 容易证明下述两个定理.

【定理 5-11】 (1) 小于5个元素的格为分配格.

(2) 任意链是分配格.

【定理 5-12】 设$(L,\leqslant)$是格,则 L 是分配格的充要条件是对于任意 $x,y,z\in L$,由 $x+y=x+z$ 和 $x\cdot y=x\cdot z$ 可以推出 $y=z$.

5.4.3 有补格

一般来说,格 L 不一定存在最大元与最小元. 例如,实数集 $\mathbf{R}$ 关于数的小于等于关系$\leqslant$

所作成的格$(\mathbf{R}, \leqslant)$.

【定义 5-24】 设$(L,\leqslant)$是格，若 L 存在最大元素以及最小元素，则称$(L,\leqslant)$为**有界格**(bounded lattice).

按偏序集中的约定：有界格的最大元素记为 1，最小元素记为 0. 根据定义知，在有界格$(L,\leqslant)$中，对任意 $x\in L$，有 $0\leqslant x\leqslant 1$. 进而有 $x+1=1, x\cdot 1=x, x+0=x, x\cdot 0=0$，于是有界格 L 关于"$\cdot$"运算有乘法幺元 1，L 关于"$+$"运算有加法幺元 0.

【例 5-33】 证明：对任意集合 X，$(P(X),\subseteq)$是有界格.

证 由于$\varnothing$，$X\in P(X)$，且对于任意 $A\in P(X)$均有$\varnothing\neq A\subseteq X$，所以$(P(X),\subseteq)$的最大元为 X，最小元为$\varnothing$. 因此$(P(X),\subseteq)$是有界格.

显然，任意有限格是有界格.

【定义 5-25】 设$(L,+,\cdot)$是有界格，$a\in L$，若存在 $b\in L$ 使得 $a+b=1$ 且 $a\cdot b=0$，则称 b 为 a 的**补元**(complement).

显然，在任意有界格中，若 b 为 a 的补元，则 a 为 b 的补元；0 与 1 互为补元. 但对于有界格，不是每个元素均有补元，同时一个元素的补元未必唯一.

【例 5-34】 对于哈斯图如图 5-6 所示的格，讨论每个元素的补元.

解 0 与 1 互为补元. a 的补元为 d. b 的补元不存在. c 的补元为 e. d 的补元为 a 和e. e 的补元为 c 和 d.

图 5-6

【定义 5-26】 设$(L,+,\cdot)$是有界格，若 L 中每个元素都有补元，则称$(L,+,\cdot)$为**有补格**(lattice complemented).

【例 5-35】 证明：对任意集合 X，$(P(X),\subseteq)$是有补格.

证 因为$(P(X),\subseteq)$是有界格，而对于任意 $A\in P(X)$，取 $X-A\in P(X)$，由于 $A\cup(X-A)=X$ 且 $A\cap(X-A)=\varnothing$，所以 $A\in P(X)$有补元，因此$(P(X),\subseteq)$是有补格.

同样，$(F,\Rightarrow)$也是有补格，其中 F 是所有合式公式组成的集合，$\Rightarrow$是公式间的逻辑蕴涵关系.

【定理 5-13】 在分配格中，若一个元素存在补元，则补元是唯一的.

证 设$(L,\leqslant)$是有界分配格，$a\in L$，b 和 c 是 a 的补元，则

$$a+b=1, a\cdot b=0$$
$$a+c=1, a\cdot c=0$$

于是 $a+b=a+c, a\cdot b=a\cdot c$，由分配格的性质知 $b=c$.

根据定理 5-13 知，在有补分配格中，每个元素都有唯一的补元. 正因为如此，在有补分配格中可以定义一个元素的补运算"$\overline{\ }$"，它是其上的 1 元代数运算. 显然，在有补分配格中$\overline{0}=1, \overline{1}=0$ 且对于任意 $x\in L$ 有 $\overline{\overline{x}}=x$.

下述定理是有补分配格的重要性质.

【定理 5-14】 设$(L,\leqslant)$是有补分配格，则 De Morgan 律成立，即对于任意 $x,y\in L$ 有：

(1) $\overline{x+y}=\overline{x}\cdot\overline{y}$；

(2) $\overline{x\cdot y}=\overline{x}+\overline{y}$.

证 (1) 由于

$$(x+y)+(\overline{x}\cdot\overline{y})=((x+y)+\overline{x})\cdot((x+y)+\overline{y})$$

$$=((x+\bar{x})+y)\cdot(x+(\bar{y}+y))$$
$$=(1+y)\cdot(x+1)=1\cdot 1=1,$$

并且

$$\begin{aligned}(x+y)\cdot(\bar{x}\cdot\bar{y})&=(x\cdot(\bar{x}\cdot\bar{y}))+(y\cdot(\bar{x}\cdot\bar{y}))\\&=((x\cdot\bar{x})\cdot\bar{y})+(\bar{x}\cdot(\bar{y}\cdot y))\\&=(0\cdot\bar{y})+(\bar{x}\cdot 0)=0+0=0,\end{aligned}$$

所以$\overline{x+y}=\bar{x}\cdot\bar{y}$.

(2) 类似于(1)的证明.

5.4.4 布尔代数

【定义 5-27】 元素个数≥2 的有补分配格$(B,\leqslant)$称为**布尔代数**(Boolean algebra)或**布尔格**.

如图 5-7 所示是偏序集与各种格之间的相互关系.

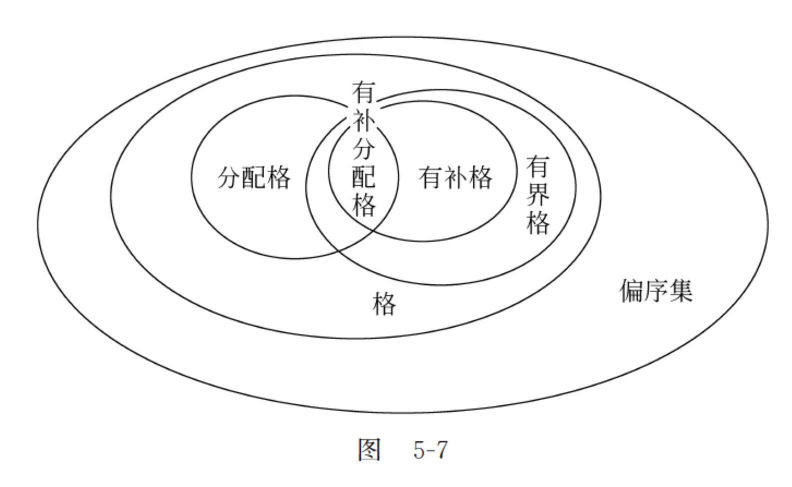


图 5-7

仅 1 个元素的有补分配格是布尔代数的退化情形,一般不作为布尔代数考虑,可参见布尔代数的公理化定义.

显然,在任何布尔代数或布尔格中有两个特殊元素,一个是其最小元 0,一个是其最大元 1. 当然 $0\neq 1$.

由前面的讨论知,在任意布尔代数$(B,\leqslant)$中可以定义 3 种代数运算:对于任意 x,$y\in B$.

(1) 布尔加"+":$x+y=\sup\{x,y\}$.

(2) 布尔乘"·":$x\cdot y=\inf\{x,y\}$.

(3) 布尔补"¯":$\bar{x}=x$ 的补元.

【例 5-36】 设$|X|\geqslant 1$,证明$(P(X),\subseteq)$是布尔代数,称$(P(X),\subseteq)$为**集合代数**.

证 由于$(P(X),\subseteq)$既是有补格又是分配格,在$|X|\geqslant 1$时$(P(X),\subseteq)$是布尔代数.

同理,所有 A 到 B 的关系组成的集合 $\mathscr{R}$ 关于包含关系"⊆"构成布尔代数$(\mathscr{R},\subseteq)$,称为**关系代数**.

【例 5-37】 证明:$(F,\Rightarrow)$是布尔代数,其中 F 是所有合式公式组成的集合,⇒是公式间的逻辑蕴涵关系,称$(F,\Rightarrow)$为**逻辑代数**.

证　由于$(F,\Rightarrow)$既是有补格又是分配格，而$0,1\in F$，所以$(F,\Rightarrow)$是布尔代数.

特别地，令G是所有命题公式组成的集合，则$(G,\Rightarrow)$称为**命题代数**. 令H是仅含命题变元$p_1,p_2,\cdots,p_n$的所有命题公式组成的集合，则$(H,\Rightarrow)$是布尔代数，这时$|H|=2^{2^n}$.

由例5-36和例5-37知，集合代数和逻辑代数都是布尔代数，因此它们有完全相似的性质.

【定理5-15】　设$(B,\leqslant)$是布尔代数，则对于任意$x,y,z\in B$.

因为$(B,\leqslant)$是格，所以有

(1) $x\leqslant x+y=\sup\{x,y\}$，$y\leqslant x+y=\sup\{x,y\}$，

$x\cdot y=\inf\{x,y\}\leqslant x$，$x\cdot y=\inf\{x,y\}\leqslant y$；

(2) 对偶原理成立；

(3) **保序性**　对于任意$x_1,x_2,y_1,y_2\in L$，若$x_1\leqslant y_1$且$x_2\leqslant y_2$，则$x_1+x_2\leqslant y_1+y_2$且$x_1\cdot x_2\leqslant y_1\cdot y_2$；

(4) **幂等性**　$x+x=x$，$x\cdot x=x$；

(5) **交换性**　$x+y=y+x$，$x\cdot y=y\cdot x$；

(6) **结合性**　$(x+y)+z=x+(y+z)$，$(x\cdot y)\cdot z=x\cdot(y\cdot z)$；

(7) **吸收性**　$x+(x\cdot y)=x$，$x\cdot(x+y)=x$；

(8) $x\leqslant y\Leftrightarrow x+y=y\Leftrightarrow x\cdot y=x$；

因为$(B,\leqslant)$是分配格，所以有

(9) **分配性**　$x\cdot(y+z)=(x\cdot y)+(x\cdot z)$，$x+(y\cdot z)=(x+y)\cdot(x+z)$；

(10) 若$x+y=x+z$且$x\cdot y=x\cdot z$，则$y=z$；

因为$(B,\leqslant)$是有补格，所以有

(11) $0\leqslant x\leqslant 1$；

(12) **幺元**　B关于"·"运算有乘法幺元1，B关于"+"运算有加法幺元0；

因为$(B,\leqslant)$是有补分配格，所以有

(13) **有补律**　$a+\overline{a}=1$，$a\cdot\overline{a}=0$；

(14) **对合律**　$\overline{\overline{x}}=x$；

(15) **De Morgan律**　$\overline{x+y}=\overline{x}\cdot\overline{y}$，$\overline{x\cdot y}=\overline{x}+\overline{y}$；

(16) $x\leqslant y\Leftrightarrow x\cdot\overline{y}=0\Leftrightarrow\overline{x}+y=1$.

以下是布尔代数的特征性质

(1) 交换律　$x+y=y+x$，$x\cdot y=y\cdot x$.

(2) 分配律　$x\cdot(y+z)=(x\cdot y)+(x\cdot z)$，$x+(y\cdot z)=(x+y)\cdot(x+z)$.

(3) 幺元律　$x+0=x$，$x\cdot 1=x$.

(4) 有补律　$x+\overline{x}=1$，$x\cdot\overline{x}=0$.

正因为这样，E. V. Hungtington将满足上述(1)、(2)、(3)和(4)的代数结构$(B,+,\cdot,^-,0,1)$称为布尔代数，其中$|B|\geqslant 2$. 注意，布尔代数的上述两种定义本质上相同.

显然，若X是无限集，则$(P(X),\subseteq)$是无限布尔代数. $(F,\Rightarrow)$也是无限布尔代数，其中F是所有合式公式组成的集合，$\Rightarrow$是公式间的逻辑蕴涵关系.

若$|X|=n\geqslant 1$，则$|P(X)|=2^n$，$(P(X),\subseteq)$是有限布尔代数.

两个布尔代数同构的定义类似于一般代数结构同构，下面给出**有限布尔代数**(finite

Boolean algebra)的结构定理.

【定理 5-16】 (M. H. Stone)设$(B,+,\cdot,^-,0,1)$是有限布尔代数,则存在有限集合 X 使得$(B,+,\cdot,^-,0,1)$与集合代数$(P(X),\cup,\cap,^-,\varnothing,X)$同构.

由斯通定理有以下两个推论.

推论 1 任意有限布尔代数$(B,+,\cdot,^-,0,1)$的元素个数为 2^n,其中 n 为正整数.

推论 2 在同构意义下,2^n 个元素的有限布尔代数是唯一的,其中 n 为正整数.

习 题 5.4

1. 如图 5-8 所示的哈斯图的偏序集是否是格,为什么?

2. 证明:$(\mathbf{Z}^+,|)$是格,其中 $\mathbf{Z}^+$ 是正整数集合,$|$ 是其上的整除关系.

3. 说明 $\mathbf{Z}$ 关于整除关系"$|$"不是格,但$(\mathbf{Z},\leqslant)$是格,其中$\leqslant$是数的小于等于关系.

4. 设$(L,\leqslant)$是格,对于任意 $x,y,z\in L$ 有$(x\cdot y)\cdot z=x\cdot(y\cdot z)$.

5. 设$(L,\leqslant)$是格,对于任意 $x,y\in L$ 有 $x\cdot(x+y)=x$.

6. 设$(L,\leqslant)$是格,对于任意 $x,y,z\in L$ 有$(x\cdot y)+(x\cdot z)\leqslant x\cdot(y+z)$.

7. 设$(L,\leqslant)$是格,对于任意 $a,b\in L$,若 $a\leqslant b$ 且 $a\neq b$,则记为 $a<b$. 假设 $a<b$,令 $I=\{x\mid x\in L,a\leqslant x\leqslant b\}$,则$(I,\leqslant)$是格.

8. 证明:五角格不是分配格.

9. 证明:$(F,\Rightarrow)$是分配格,其中 F 是所有合式公式组成的集合,$\Rightarrow$是公式间的逻辑蕴涵关系.

10. 证明:任意链是分配格.

11. 说明$(\mathbf{R},\leqslant)$是否是分配格,其中$\leqslant$是实数集 $\mathbf{R}$ 上的小于等于关系.

12. 证明:钻石格和五角格是有补格(如图 5-9 所示).

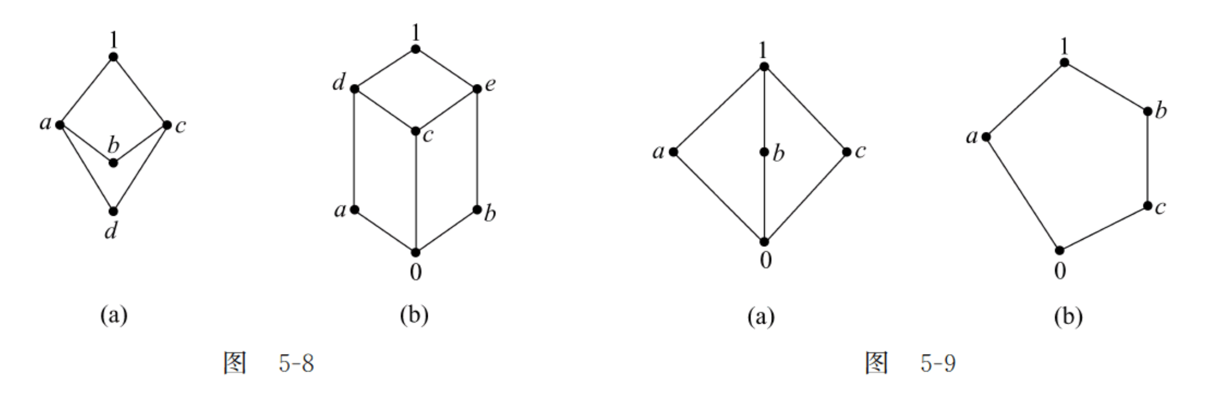


图 5-8　　　　图 5-9

13. 证明:元素个数大于等于 3 的链不是有补格.

14. 证明:$(F,\Rightarrow)$是有补格,其中 F 是所有合式公式组成的集合,$\Rightarrow$是公式间的逻辑蕴涵关系.

15. 设 n 是正整数,令 D_n 表示 n 的所有正因数组成的集合,对于整除关系"$|$",判断$(D_n,|)$是否有补格,为什么?

16. 在布尔代数$(B,+,\cdot,^-,0,1)$中,对于任意 $x,y\in B$,试证:

(1) $x+(\bar{x}\cdot y)=x+y$.

(2) $x \cdot (\bar{x} + y) = x \cdot y$.

(3) $(x \cdot y) + (x \cdot \bar{y}) = x$.

(4) $(x + y + z) \cdot (x + y) = x + y$.

17. 设$(B, +, \cdot, ^{-}, 0, 1)$是布尔代数，对于任意 $x, y, z \in B$，化简下列各式：

(1) $(1 \cdot x) + (0 \cdot \bar{y})$.

(2) $(x \cdot z) + z + ((y + \bar{y}) \cdot z)$.

(3) $\overline{x + y} + \overline{x \cdot y}$.

(4) $(\bar{x} \cdot \bar{y} \cdot z) + (x \cdot \bar{y} \cdot z) + (x \cdot \bar{y} \cdot \bar{z})$.

本 章 小 结

1. 代数结构

前面几章分别讨论的是集合代数、关系代数和逻辑代数．一个集合 A 及 A 上的封闭运算 $f_1, f_2, \cdots, f_k(k \geqslant 1)$就构成代数结构$(A, f_1, f_2, ..., f_k)$．对于特定的代数结构，一般要求其中的运算具有某种性质.

设 $*$ 是非空集合 S 上的 2 元代数运算，若 $*$ 满足结合律，则$(S, *)$就是半群．设 $*$ 是非空集合 M 上的 2 元代数运算，若 $*$ 满足结合律且 M 关于 $*$ 有幺元 e，则$(M, *, e)$就是独异点.

子代数一般比原来的代数结构要“小”．讨论代数结构，一种常用的方法是根据其子代数所具有的性质去推测原代数的性质.

借助于映射可以讨论两个代数结构之间的关系：代数结构的同态与同构，这是讨论代数结构的又一种常用的方法.

了解代数结构的定义、子代数和代数结构的同态与同构，理解半群和独异点的定义.

2. 群的定义及性质

设 G 是非空集合，$\cdot$ 是 G 上的 2 元代数运算，$(G, \cdot)$是群必须满足下列 3 个条件.

(1) $\cdot$ 满足结合律：$\forall x, y, z \in G, (x \cdot y) \cdot z = x \cdot (y \cdot z)$；

(2) G 关于 $\cdot$ 有单位元，通常记为 e：$\forall x \in G, x \cdot e = e \cdot x = x$；

(3) G 中每一个元素在 G 中都有逆元：$\forall x \in G, \exists x^{-1} \in G, x \neg x^{-1} = x^{-1} \cdot x = e$.

例如，$(\mathbf{R}, +)$，$(\mathbf{R} - \{0\}, \cdot)$是群.

运算可交换的群是交换群或阿贝尔群．非阿贝尔群的最小阶是 6，例如 $A = \{1, 2, 3\}$ 上的所有置换构成的集合 S_3 关于映射的复合运算$\circ$构成的群$(S_3, \circ)$.

设$(G, \cdot)$是群，若存在 $a \in G$，使得 G 中每个元素均为 a 的某整数方幂，则称$(G, \cdot)$为循环群．重要的两类循环群：$(\mathbf{Z}_m, +_m)$是 m 阶循环群，$(\mathbf{Z}, +)$是无限循环群.

设$(G, \cdot)$是群，$\varnothing \neq H \subseteq G$，若 H 关于 G 的运算构成群，则称$(H, \cdot)$是$(G, \cdot)$的子群，记为 $H \leqslant G$.

要求掌握群的定义，理解阿贝尔群、循环群和群同态与群同构，记住：若 G 是有限群，$H \leqslant G$，则$|H| \mid |G|$.

3. 环和域

设$(R, +, \cdot)$是含两个 2 元运算的代数结构，若

(1) $(R,+)$是阿贝尔群.

(2) $(R,\cdot)$是半群.

(3) $\cdot$对$+$可分配.

则称$(R,+,\cdot)$是环.

例如，$(\mathbf{Z},+,\cdot)$，$(\mathbf{R},+,\cdot)$，$(\mathbf{Z}_m,+_m,\cdot_m)$是环.

要求掌握环的定义，理解交换环、含幺环、无零因子环、整环和除环等概念.

设$(F,+,\cdot)$是环,若$(F-\{0\},\cdot)$是 Abel 群,则称$(F,+,\cdot)$是域，例如$(\mathbf{R},+,\cdot)$，$(\mathbf{Z}_p,+_p,\cdot_p)$(其中 p 为素数).

有限域的几个结论成立：

(1) 设$(F,+,\cdot)$是有限域,则存在素数 p 和正整数 n 使得$|F|=p^n$.

(2) 对于任意素数 p 和正整数 n,存在 p^n 个元素的有限域.

(3) 元素个数相同的有限域是同构的.

要求掌握域的定义，记住有限域的上述 3 个结论.

4. 格与布尔代数

设$(L,\leqslant)$是偏序集,若 L 中任意两个元素都存在上确界以及下确界,则称$(L,\leqslant)$是格. 格$(L,\leqslant)$中的运算满足(1)交换性，(2)结合性,(3)吸收性.

设$(L,\leqslant)$是格,若格中运算相互可分配,则称格$(L,\leqslant)$为分配格.

设$(L,+,\cdot)$是有界格,若 L 中每个元素 $a\in L$,存在 $b\in L$ 使得 $a+b=1$ 且 $a\cdot b=0$,则称$(L,+,\cdot)$为有补格.

元素个数$\geqslant 2$ 的有补分配格$(B,\leqslant)$称为布尔代数. 例如$(P(X),\subseteq)$，$(\Re,\subseteq)$，$(F,\Rightarrow)$是布尔代数.

设$(L,\leqslant)$是有补分配格,则 De Morgan 律成立,即对于任意 $x,y\in L$ 有

(1) $\overline{x+y}=\overline{x}\cdot\overline{y}$. (2)$\overline{x\cdot y}=\overline{x}+\overline{y}$.

Stone 定理 设$(B,+,\cdot,\overline{\ },0,1)$是有限布尔代数,则存在有限集合 X 使得$(B,+,\cdot,\overline{\ },0,1)$与集合代数$(P(X),\cup,\cap,\overline{\ },\varnothing, X)$同构，进而

(1) 任意有限布尔代数$(B,+,\cdot,\overline{\ },0,1)$的元素个数为 2^n,其中 n 为正整数.

(2) 在同构意义下,2^n 个元素的有限布尔代数是唯一的,其中 n 为正整数.

要求掌握格的定义，理解格的运算和运算性质. 掌握分配格、有补格和布尔代数的定义，理解格、分配格、有补格、布尔代数的有关性质，记住有限布尔代数的 Stone 定理及其推论.

第 6 章　图　　论

图论的创始人是瑞士数学家 L. Euler,他于 1736 年首次建立“图”模型解决了哥尼斯堡七桥问题.

1936 年匈牙利的 Deneskönig 出版了第一本图论方面的专著,在这期间德国的 G. R. Kirchhoff,英国的 A. Cayley 和 W. R. Hamilton 以及法国的 M. E. C. Jordan 等人都做出过开创性的工作.

将集合间的关系画图表示出来就是图. 图论讨论的是“拓扑结构”,涉及集合、映射、运算和关系等,其应用领域非常广泛,它已经渗透到诸如语言学、逻辑学、物理学、化学、电信工程、信息论、控制论、经济管理等各个领域,特别是在计算机科学中的数据结构、计算机网络、计算机软件、算法理论、操作系统、分布式系统、编译程序以及数据挖掘等方面都扮演着重要角色.

实际上,数据库和软件工程中的 E-R 图, Internet、WWW 和社会网络等复杂网络研究都要用到较深入的图论知识,计算机算法很多都是归结到图论算法进行研究的.

6.1　图的基本概念

6.1.1　图的定义

哥尼斯堡(Köningsberg)城位于立陶宛的普雷格尔(Pregel)河畔,河中两个岛将整个城市分成了 4 部分,各部分由 7 座桥连接,如图 6-1(a)所示. 问题是: 是否可从某一个地方出发,经过 7 座桥,每座桥只经过一次,然后又回到原出发点. 这是一个久而不得其解的问题,当时的 L. Euler 是这样做的: 将 4 个地方分别用 4 个点(顶点、节点或结点)A,B,C,D 来表示,两个地方之间有一座桥直接相连就在相应的两个点之间画一条“边”,如图 6-1(b)所示,于是就得到一个图,这是七桥问题的图模型.

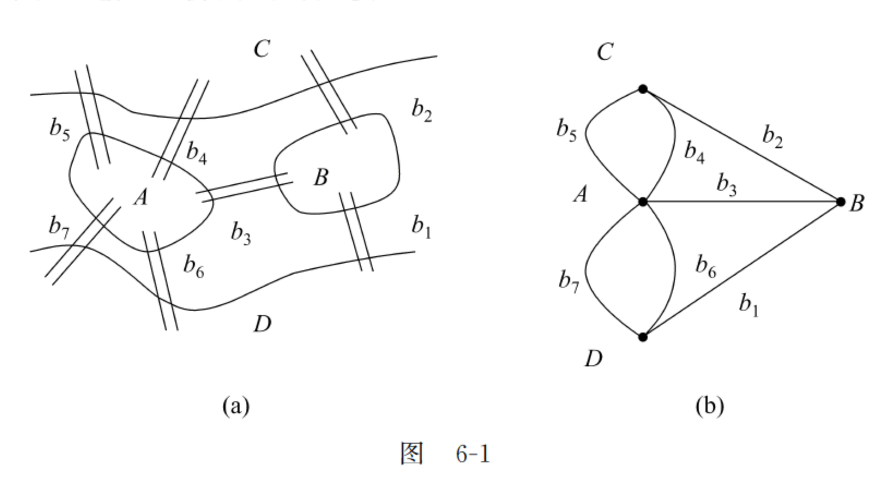


图　6-1

假定有 5 个程序,分别是 v_1,v_2,v_3,v_4,v_5,它们之间的调用关系如图 6-2 所示,其中 e_1

表示 v_2 可以调用 v_1，e_2 表示 v_1 可以调用 v_2，e_4 表示 v_5 可以调用自身 v_5，e_9 表示 v_4 可以调用 v_3 等.

由前面的 2 个例子可以得出：

【定义 6-1】 **图** G(graph)主要由如下两部分组成.

(1) 节点集合 V，其中的元素 v 称为**节点**(vertex 或 node).

(2) 边集合 E，其中的元素称为**边**(edge).

通常将图 G 记为 $G=(V,E)$.

需要说明如下：

① 节点又可以称为点、顶点或结点，常用一个实心点或空心点表示，但在实际应用中还可以用诸如方形、圆形、菱形等符号，为了方便可以在这些符号的旁边或内部写上表意名称，或直接用表意名称代表点，如图 6-3 所示是一个典型的**贝叶斯网络**(Bayesian networks).

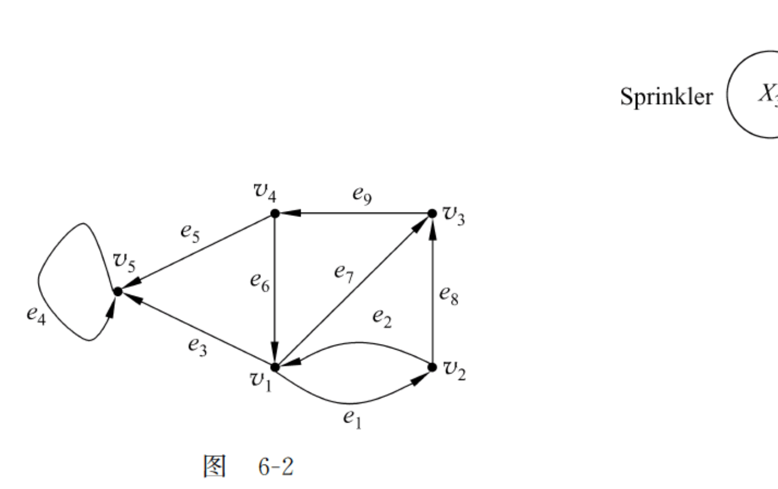


图 6-2

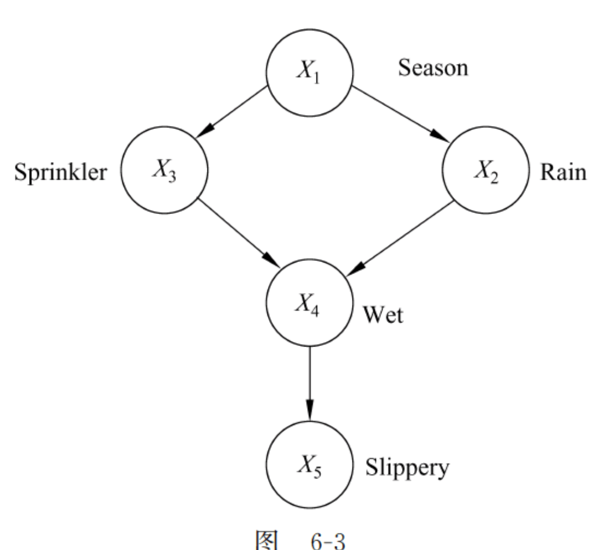


图 6-3

② 边及其表示. 在图 6-1(b)中的边如 b_3，是没有方向的，称为**无向边**，可以认为 A 是起点，B 是终点，也可以认为 B 是起点，A 是终点，这时 A 和 B 称为边 b_3 的**端点**(endvertices)，在不致混淆时可将边 b_3 简记为 AB、BA、$\{A,B\}$或$\{B,A\}$，表示边的集合$\{A,B\}=\{B,A\}$中的两元素可以相同，是可重集合，与通常的集合有所不同. 在图 6-2中的边如 e_8 有方向，称为**有向边**或**弧**(arc)，其起点(弧尾)为 v_2，其终点(弧头)为 v_3，其两个端点分别为 v_2 和 v_3，在方便时可用有序对(v_2,v_3)或$\langle v_2,v_3\rangle$表示边 e_8.

所有边都是无向边的图称为**无向图**(graph 或 undirected graph)，所有边都是有向边的图称为**有向图**(digraph 或 directed graph). 我们暂不讨论既有无向边又含有向边的混合图，同时假定图 $G=(V,E)$中的 V 和 E 均有限.

③ 图的拓扑不变性质. 需要注意的是，我们讨论的图不但与节点位置无关，而且与边的形状和长短也无关.

有 n 个节点的图称为 **n 阶图**，有 n 个节点 m 条边的图称为 **(n, m) 图**. 如图 6-4(a)和图 6-4(b)所示的图分别是 3 阶无向图和 4 阶有

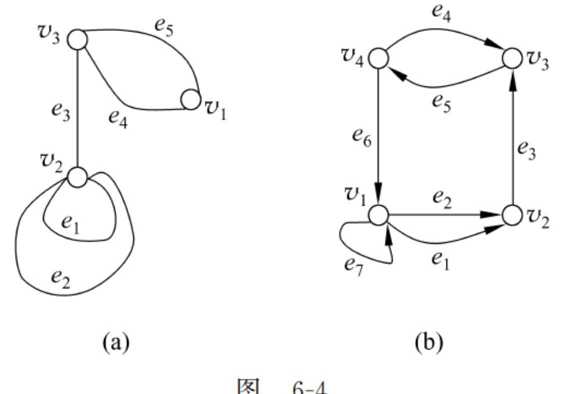


图 6-4

向图.

在图 $G=(V,E)$ 中,称 $V=\varnothing$ 的图为**空图**(empty graph),记为 $\varnothing$,若 $V\neq\varnothing$ 但 $E=\varnothing$ 的图称为**零图**(discrete graph),n 阶零图可记为 N_n,仅一个节点的零图称为**平凡图**(trivial graph).

思考 图的计算机表示方法.

6.1.2 邻接

【定义 6-2】 设 $G=(V,E)$ 是图,对于任意 $u,v\in V$,若从节点 u 到节点 v 有边,则称 u 是**邻接到 v**(adjacent to)或称 u 和 v 是**邻接的**(adjacent).

在无向图中,若 u 和 v 是邻接的,则 v 和 u 也是邻接的. 但需要注意,在有向图中,由 u 和 v 邻接不能得出 v 和 u 邻接,例如在图 6-4(b)中,节点 v_4 与节点 v_1 邻接,但节点 v_1 与 v_4 不邻接. 因此,邻接与节点的次序有关. 同时,在图 6-4(a)中,v_2 与 v_2 是邻接的,但 v_1 与 v_1 以及 v_3 与 v_3 是不邻接的,在图 6-4(b)中,v_1 与 v_1 是邻接的,而 v_i 与 v_i 是不邻接的,$2\leqslant i\leqslant 4$.

在有向图 $G=(V,E)$ 中,若 u 邻接到 v,则称 u 是 v 的**先驱元素**,v 是 u 的**后继元素**.

在无向图 $G=(V,E)$ 中,若两条边 e_1 和 e_2 有公共端点,则称**边 e_1 和 e_2 是邻接的**.

6.1.3 关联

【定义 6-3】 设 $G=(V,E)$ 是图,$e\in E$,e 的两个端点分别为 u 和 v,则称边 e 与节点 u 以及边 e 与节点 v 是**关联**的(incident).

显然,图的任意一条边都关联两个节点. 关联相同两个节点的边称为**自环**,可简称**环**(loop). 关联的起点相同与终点也相同的边称为**多重边**(multiple edges)或平行边,其边数称为边的**重数**(multiplicity).

在图 6-4(a)中,在节点 v_2 处有两个自环 e_1 和 e_2,它们是多重边,e_4 和 e_5 是多重边. 在图 6-4(b)中,在节点 v_1 处有 1 个自环 e_7,e_1 和 e_2 是多重边,但 e_4 和 e_5 不是多重边.

6.1.4 简单图

1. 简单图

【定义 6-4】 设 $G=(V,E)$ 是图,若 G 中既无自环又无多重边,则称 G 是**简单图**(simple graph).

在前面所出现的图中,只有图 6-3 是简单图. 如图 6-5 所示是**彼得森**(Petersen,1831—1910)**图**,它是一个有着特殊性质的简单图,一种**妖怪图**(snark graph),后面会多次出现.

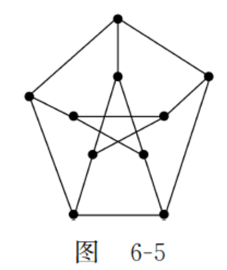


图 6-5

2. 完全无向图

【定义 6-5】 设 $G=(V,E)$ 是 n 阶简单无向图,若 G 中任意节点都与其余 $n-1$ 个节点邻接,则称 G 为 n 阶**完全无向图**(Complete Graph),记为 K_n.

图 6-6(a)～图 6-6(c)所示分别是 K_3,K_4 和 K_5.

将 n 阶完全无向图 K_n 的边任意加一个方向所得到的有向图称为 n 阶**竞赛图**.

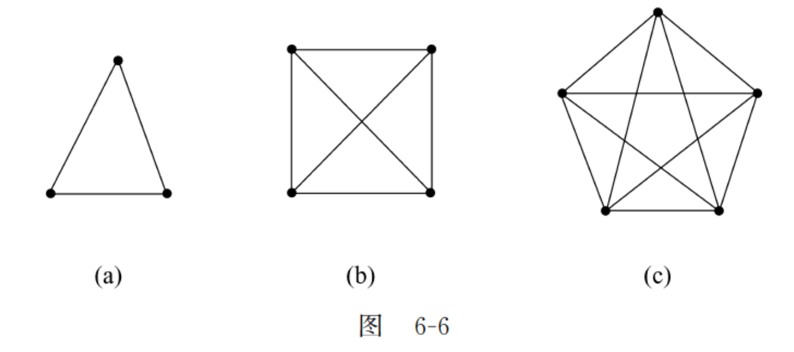

(a)　(b)　(c)

图 6-6

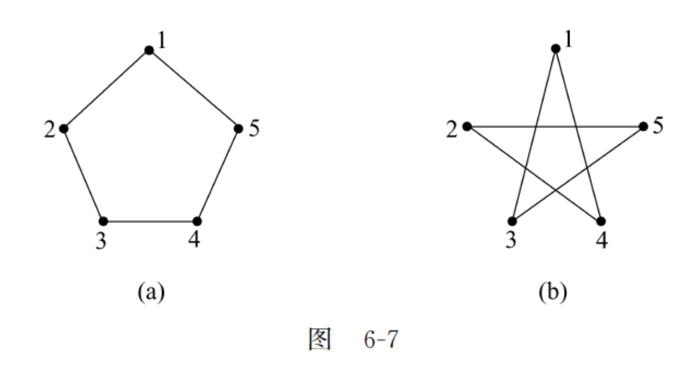
设 $G=(V,E)$ 是 n 阶简单有向图，若 G 中任意节点都与其余 $n-1$ 个节点邻接，则称 G 为 n 阶**完全有向图**. 显然，n 阶完全有向图 K_n 的任意两个节点都是相互邻接的，其边是成对出现的.

容易证明，n 阶完全无向图 K_n 的边数为 $n(n-1)/2$.

3. 补图

【定义 6-6】 设 $G=(V,E)$ 是 n 阶简单无向图，由 G 的所有节点以及由能使 G 成为 K_n 需要添加的边构成的图称为 G 的**补图**(complementary graph)，记为 $\overline{G}$.

如图 6-7(a)和图 6-7(b)所示的图互为补图，它们是相对于完全图而言的.



(a)　(b)

图 6-7

显然，对于任意节点 u 和 v，若 u 和 v 在 G 中不邻接，则 u 和 v 在 $\overline{G}$ 中邻接；若 u 和 v 在 G 中邻接，则 u 和 v 在 $\overline{G}$ 中不邻接.

习　题　6.1

1. 在图 6-8 中，用 1，2，3，4，5，6 表示 6 个人，两个点之间的无向边表示所对应的两个人认识，则图 6-8 所示的含义是什么？能得出任意 6 个人中有 3 个人相互认识或相互不认识的结论吗？

2. 在一次 10 周年同学会上，想统计所有人握手的次数之和，应该如何建立该问题的图模型？

3. 在一次联欢舞会上，要得出跳了奇数次舞的人数的规律，应该如何建立图模型？特别地，一个人单独跳一曲舞该如何处理呢？某两人多次跳舞又如何处理？

图 6-8

4. 对于任意 $n(n\geqslant 2)$ 个人的组里，必有两个人有相同个数的朋友，解答此问题的图模

型该如何建立?

5. (**3户3井问题**)在一个地方有3户人家,并且有3口井供他们使用.由于土质和气候的关系,有些井中的水常常干枯,因此各户人家要到有水的井去打水.不久,这3户人家成了冤家,于是决定各自修一条路通往水井,打算使得他们在去水井的路上不会相遇.试建立解决此问题的图模型.

6. (**过河问题**)某人挑一担菜并带一条狼和一只羊要从河的一岸到对岸去.由于船太小,只能带狼、菜、羊中的一种过河.由于明显的原因,当人不在场时,狼要吃羊,羊要吃菜.通过建立图模型给出问题答案.

7. (**分油问题**)有3个油桶A,B,C,分别可装8斤、5斤和3斤油.假设A桶已经装满了油,在没有其他度量工具的情况下,要将油平分,试通过建立图模型给出问题答案.

8. 证明:任何n阶完全图K_n的边数为$n(n-1)/2$.

9. 对于n阶简单无向图G,若其边数为m,试计算G的补图$\overline{G}$的边数.

10. 举出两个已经遇到的应用图的例子.

6.2 节点的度数

在"七桥问题"中,图6-1(b)的图中一个节点的度数就是图6-1(a)的相应地点出发的"桥"的数目.

在任意图$G=(V,E)$中,每一条边$e\in E$都要关联2个端点$u\in V$和$v\in V$.若$u=v$,则称边e与节点v的关联次数为2;若$u\neq v$,则称边e与节点v的关联次数为1.若边$e\in E$与节点$v\in V$不关联,则称边e与节点V的关联次数为0.

【定义6-7】 设$G=(V,E)$是无向图,$v\in V$,称与节点v关联的所有边的关联次数之和为节点v的**度数**(degree),记为$\deg(v)$.

在图6-9(a)中,$\deg(v_1)=2$,$\deg(v_2)=5$,$\deg(v_3)=3$.很容易知道,节点处的一个自环算2度.

【定义6-8】 设$G=(V,E)$是有向图,$v\in V$,称以v为起点的边的数目为节点v的**出度**(out-degree),记为$\mathrm{od}(v)$,以v为终点的边的数目为节点v的**入度**(in-degree),记为$\mathrm{id}(v)$,称$\mathrm{od}(v)+\mathrm{id}(v)$为节点$v$的**度数**,记为$\deg(v)$.

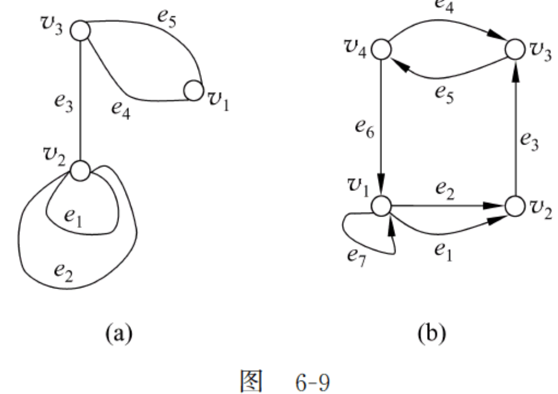


图 6-9

在图6-9(b)中,节点v_1,v_2,v_3和v_4的出度分别为3,1,1,2,入度分别为2,2,2,1,于是其度数分别为5,3,3,3.在有向图中,同样有节点处的一个自环算2度.

下面的定理是L. Euler在1736年证明的图论中的第一定理,常称为"握手定理",因为一条边表示两只手握在一起.

【定理6-1】 在任何(n,m)图$G=(V,E)$中,其所有节点度数之和等于边数m的2倍,即

$$\sum_{v \in V} \deg(v) = 2m$$

证 这是由于每一条边在计算 $\sum_{v \in V} \deg(v)$ 时都是占 2 度，结论成立.

由上述定理容易得出

推论 在任意图中，度数为奇数的节点个数必为偶数.

证 因为 $\sum_{v \in V} \deg(v) = 2m$，而 $\sum_{v \in V} \deg(v) = \sum_{\deg(v)\text{是偶数}} \deg(v) + \sum_{\deg(v)\text{是奇数}} \deg(v)$，所以 $\sum_{\deg(v)\text{是奇数}} \deg(v)$ 必为偶数，进而度数为奇数的节点个数必为偶数.

由定理 6-1 及其推论很容易知道，在任何一次聚会上，所有人握手次数之和必为偶数并且握了奇数次手的人数必为偶数.

在任意有向图中，显然有：

【定理 6-2】 在任意有向图中，所有节点的出度之和等于入度之和.

在任意图 $G=(V,E)$ 中，度数为 0 的节点称为**孤立点**(isolated vertex)，度数为 1 的节点称为**悬挂点**(pendant vertex).

【例 6-1】 证明：对于任意 $n(n \geqslant 2)$ 个人的组里，必有两个人有相同个数的朋友.

证 将组里的每个人看作节点，两个人是朋友当且仅当对应的节点邻接，于是得到一个 n 阶简单无向图 G，进而 G 中每节点的度数可能为 $0,1,2,\cdots,n-1$ 中一个.

当 G 中无孤立点时，于是每节点的度数可能为 $1,2,\cdots,n-1$. 由于共有 n 个节点，于是必有两节点度数相同.

当 G 中有孤立点时，这时每节点的度数只可能为 $0,1,2,\cdots,n-2$. 同样由于共有 n 个节点，因此必有两节点度数相同.

若一个简单无向图 G 的每节点度数均为 k，则称 G 为 ***k*-正则图**(k-regular graph). 图 6-10(a)和图 6-10(b)是两个 3-正则(6,9)图.

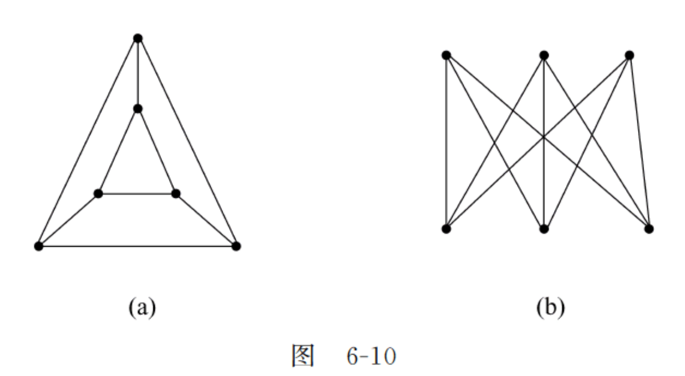


图 6-10

【例 6-2】 设无向图 G 是一个 3-正则(n,m)图，且 $2n-3=m$，求 n 和 m 各是多少？

解 由握手定理有 $3n=2m$. 根据已知，$2n-3=m$，可以得出 $n=6$，$m=9$. 这样的图可如图 6-10 所示.

【定义 6-9】 在任意图 $G=(V,E)$ 中，称 $\Delta(G)=\max_{v \in V} \deg(v)$ 为图 G 的**最大度**，$\delta(G)=\min_{v \in V} \deg(v)$ 为图 G 的**最小度**. 在有向图 $G=(V,E)$ 中，称 $\Delta^{+}(G)=\max_{v \in V} \mathrm{od}(v)$ 为有向图 G 的**最大出度**，$\delta^{+}(G)=\min_{v \in V} \mathrm{od}(v)$ 为图 G 的**最小出度**，$\Delta^{-}(G)=\max_{v \in V} \mathrm{id}(v)$ 为有向图 G 的**最大入度**，$\delta^{-}(G)=\min_{v \in V} \mathrm{id}(v)$ 为图 G 的**最小入度**.

在图 6-9(a)中，$\Delta(G)=5$，$\delta(G)=2$. 在图 6-9(b)中，$\Delta(G)=5$，$\delta(G)=3$. 对于正则图有 $\Delta(G)=\delta(G)$.

对于无向图 $G=(V,E)$，$V=\{v_1,v_2,\cdots,v_n\}$，称 $\deg(v_1),\deg(v_2),\cdots,\deg(v_n)$ 为 G 的**度数序列**. 例如，在图 6-9(a)中图的度数序列为 2，5，3. 对于有向图，还可以定义其出度序列和入度序列.

【例 6-3】 是否存在一个无向图，其度数序列分别为：

(1) 7，5，4，2，2，1.

(2) 4，4，3，3，2，2.

解 (1) 由于序列 7，5，4，2，2，1 中，奇数个数为奇数，根据握手定理的推论知，不可能存在一个图其度数序列为 7，5，4，2，2，1.

(2) 因为序列 4，4，3，3，2，2 中，奇数个数为偶数，可以得到一个无向图如图 6-11 所示，其度数序列为 4，4，3，3，2，2.

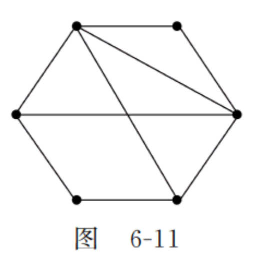
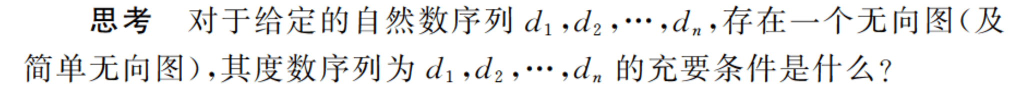


图 6-11

思考 对于给定的自然数序列 $d_1,d_2,\cdots,d_n$，存在一个无向图(及简单无向图)，其度数序列为 $d_1,d_2,\cdots,d_n$ 的充要条件是什么?



习 题 6.2

1. 证明：对于任意 n 阶简单图 G 有 $\Delta(G)\leqslant n-1$.

2. 无向图 G 有 6 条边，各有一个 3 度和 5 度节点，其余均为 2 度节点，求 G 的阶数.

3. 证明：

(1) 3-正则图的阶必为偶数.

(2) 有 n 个人，每个人恰有 3 个朋友，则 n 是偶数.

4. 将有向图 G 的边的方向去掉得到的无向图称为 G 的**基础图**，基础图是完全图的有向图称为**竞赛图**. 证明：任意竞赛图的所有节点的出度平方和等于入度平方和.

5. 若 G 是(n,m)无向图，则 $\delta(G)\leqslant 2m/n\leqslant\Delta(G)$.

6. 是否存在一个无向图，其度数序列分别为

(1) 5，4，4，3，3，2，2.

(2) 4，4，3，3，2，2，2，2.

7. 画出度数序列为 3，2，2，1 的简单图和非简单图各一个.

8. 设无向图 G 有 10 条边，3 度和 4 度节点各 2 个，其余节点的度数均小于 3，则 G 至少有多少个节点? 在最少节点的情况下，求出 G 的度数序列、最大度 $\Delta(G)$和最小度 $\delta(G)$.

9. 证明：存在一个无向图 G，其度数序列为给定的自然数序列 $d_1,d_2,\cdots,d_n$ 的充要条件是 $\sum_{i=1}^{n} d_i\equiv 0(\bmod 2)$.

6.3 子图、图的运算和图同构

6.3.1 子图

可以通过一个图的子图去考察原图的有关性质以及原图的局部结构.

【定义 6-10】 设 $G=(V,E)$和 $H=(W,F)$是图，若 $W\subseteq V$ 且 $F\subseteq E$，则称 H 是 G 的子

图(subgraph).若 $H=(W,F)$ 是 $G=(V,E)$ 的子图且 $W=V$,则称 H 是 G 的**生成子图**(spanning subgraph).

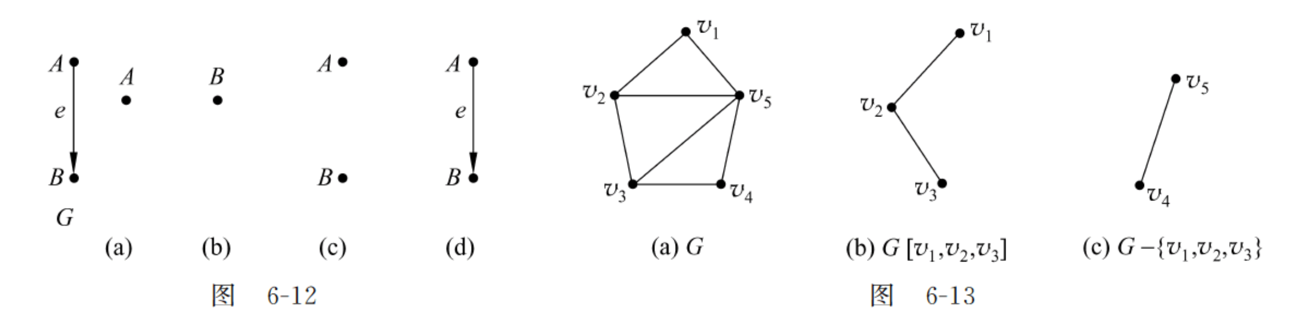
【例 6-4】 求出如图 6-12 所示中有向图 G 的所有子图.

解 G 的所有子图除空图 $\varnothing$ 外分别为图 6-12(a)～图 6-12(d),其中图 6-12(c)和图6-12(d)是 G 的生成子图.

常见的 4 种产生 $G=(V,E)$ 的子图的方式(也是图的 4 种运算)如下:

(1) $G[W]$ 设 $W\subseteq V$,则以 W 为节点集合,以两端点均属于 W 的所有边为边集合构成的子图,称为**由 W 导出的子图**(induced subgraph by W),记为 $G[W]$.

图 6-13(b)是图 G 中节点集合 $W=\{v_1,v_2,v_3\}$ 所导出的子图.



(a) (b) (c) (d)

图 6-12

(a) G (b) $G[v_1,v_2,v_3]$ (c) $G-\{v_1,v_2,v_3\}$

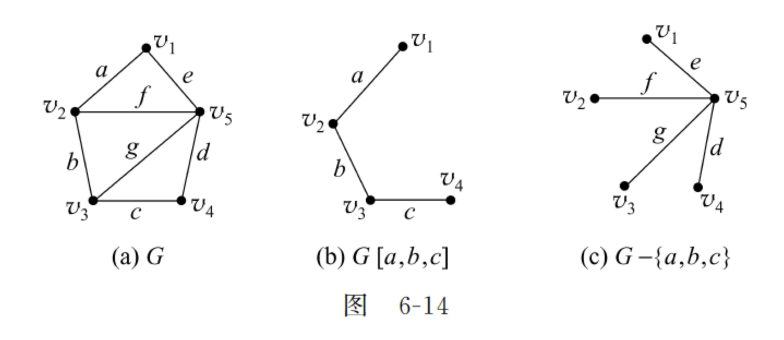
图 6-13

(2) $G-W$ 设 $W\subseteq V$,导出子图 $G[V-W]$ 记为 $G-W$,是在 G 中去掉所有 W 中的节点,同时也要去掉与 W 中节点关联的所有边.通常将 $G-\{v\}$ 记为 $G-v$.

图 6-13(c)是从图 G 中去掉节点集合 $W=\{v_1,v_2,v_3\}$ 所得到的子图.

(3) $G[F]$ 设 $F\subseteq E$,则以 F 为边集合,以 F 中边的所有端点为节点集合构成的子图,称为**由 F 导出的子图**(induced subgraph by F),记为 $G[F]$.

图 6-14(b)是图 G 中边集合 $W=\{a,b,c\}$ 所导出的子图.



(a) G (b) $G[a,b,c]$ (c) $G-\{a,b,c\}$

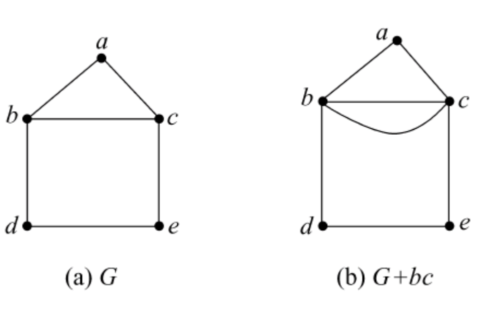
图 6-14

(4) $G-F$ 设 $F\subseteq E$,则从 G 中去掉 F 中的所有边得到的生成子图记为 $G-F$.

图 6-14(c)是从图 G 中去掉 $F=\{a,b,c\}$ 中的所有边得到的生成子图 $G-\{a,b,c\}$.

设 $G=(V,E)$ 是 n 阶简单无向图,则 G 的补图为 $\overline{G}=K_n-E$.

另外,也可以在图 $G=(V,E)$ 的基础之上,通过增加 V 中某些节点间的一些"新"边 U,得到一个更大的图 $G+U$.通常记 $G+\{uv\}$(或 $G+\{(u,v)\}$)为 $G+uv$(或 $G+(u,v)$).



(a) G (b) $G+bc$

图 6-15

图 6-15(b)是图 6-15(a)增加边 bc 得到的图.

6.3.2　图的运算

图的运算就是通过一定的操作，产生“新”的图. 前面的子图的产生实际上就是图的运算，但它们都是在一个图中进行讨论的.

在有些问题的讨论中，还会出现两个图之间的一些运算. 我们在此仅给出定义，请参见有关文献[16，17].

【定义 6-11】 设 $G_1=(V_1,E_1)$ 和 $G_2=(V_2,E_2)$ 是两个无向(或有向)图.

(1) 两个图的**并**(union)$G_1\cup G_2=(V,E)$，其中 $E=E_1\cup E_2$ 且 $V=V_1\cup V_2$.

(2) 两个图的**交**(cap)$G_1\cap G_2=(V,E)$，其中 $E=E_1\cap E_2$ 且 $V=V_1\cap V_2$.

(3) 两个图的**差**(difference)$G_1-G_2=(V,E)$，其中 $E=E_1-E_2$ 且 $V=V_1$.

(4) 两个图的**环和**(ring sum)$G_1\oplus G_2=(V,E)$，其中 $E=E_1\oplus E_2$ 且 $V=V_1\cup V_2$.

思考　图的每种运算的性质有哪些？它与集合的并、交、差、(补)及环和(对称差)运算的性质有什么不同？

6.3.3　图同构

由于图的拓扑性质，有可能两个表面上看起来不同的图本质上是同一个图，这就是图同构的问题.

【定义 6-12】 设 $G_1=(V_1,E_1)$ 和 $G_2=(V_2,E_2)$ 是无向(或有向)图，若存在一个双射 φ：$V_1\to V_2$ 使得对于任意 $u,v\in V_1$，$uv\in E_1$(或 $(u,v)\in E_1$)当且仅当 $\varphi(u)\varphi(v)\in E_2$(或 $(\varphi(u),\varphi(v))\in E_2$)且边的重数相同，则称图 G_1 与 G_2 **同构**(isomorphism)，记为 $G_1\cong G_2$.

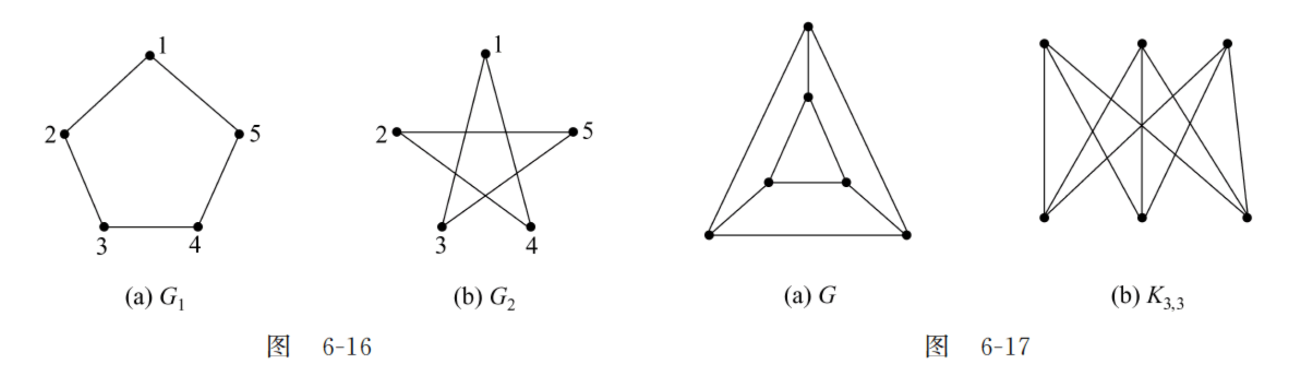
由定义知，$G_1\cong G_2$ 的充要条件是图 G_1 与 G_2 的节点与边分别存在一一对应，且保持节点与边的关联关系. 更直观地说，$G_1\cong G_2$ 是指其中一个图仅经过下列两种变换可以变为另一个图：

(1) 挪动节点的位置；

(2) 伸缩边的长短.

显然，在图 6-12 中(a)与(b)是同构的. 下列(图 6-16(a)和图 6-16(b))的两个图是同构的.

图 6-17 中的两个图是不同构的，因为(a)中图 G 含有 K_3 子图，而 $K_{3,3}$ 中没有 K_3 子图.



(a) G_1　(b) G_2

图　6-16

(a) G　(b) $K_{3,3}$

图　6-17

对于两个有向图同构的判断，特别要注意边的方向的一致性. 下列的 3 个有向图如

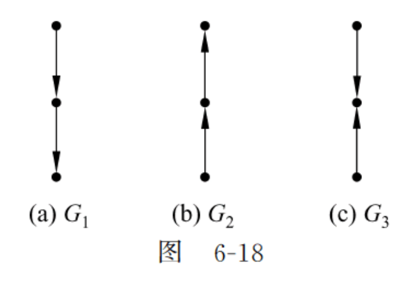


图 6-18

图 6-18所示中 $G_1 \cong G_2$，但 G_1 与 G_3 不同构，因为 G_3 中有一个节点的入度为 2，而 G_1 没有.

思考 给出至少 4 个两个图同构的必要条件.

显然，图的同构关系是等价关系，即有

(1) 自反性 对于任意图 G，有 $G \cong G$.

(2) 对称性 若 $G_1 \cong G_2$，则 $G_2 \cong G_1$.

(3) 传递性 若 $G_1 \cong G_2$ 且 $G_2 \cong G_3$，则 $G_1 \cong G_3$.

2015 年，芝加哥大学 Babai 教授给出了在拟多项式时间复杂度内判定两个图同构算法.

最后，介绍至今未解决的乌拉姆(Ulam)猜想[17].

乌拉姆(Ulam)猜想(1929) 设 G_1 和 G_2 是两个简单无向图，G_1 的节点集合 $V_1=\{v_1, v_2, \cdots, v_n\}$，$G_2$ 的节点集合 $V_2=\{w_1, w_2, \cdots, w_n\}$，若对于任意 $i=1,2,\cdots,n$，均有 $G_1-v_i \cong G_2-w_i$，则 $G_1 \cong G_2$.

乌拉姆猜想的实际模型：两张照片，用左手捂住第一张照片的一部分，右手捂住第二张照片相应的部分，能看到的部分一致. 如此轮番地观察，每次看到的图像均相同，则两张照片相同.

习 题 6.3

1. 画出 K_3 的所有不同构的非空子图.
2. 画出所有不同构的(5, 3)简单无向图及其补图.
3. 证明：在 K_4 的所有不同构的生成子图中，有 3 个具有 3 条边.
4. 证明：$n(1 \leqslant n \leqslant 3)$阶不同构的简单有向图有 20 个.
5. 说明图 6-19(a)和图 6-19(b)两个无向图不同构.

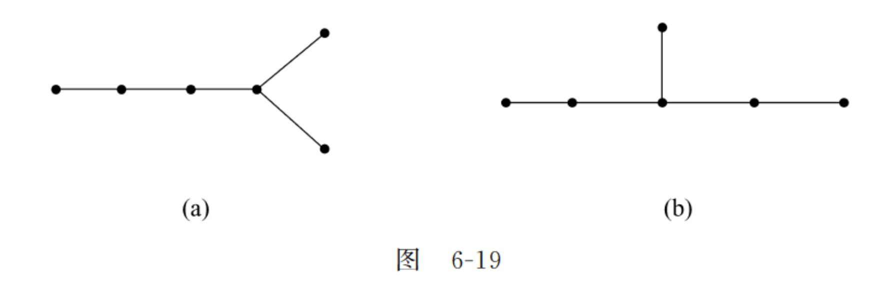


图 6-19

6. 说明图 6-20 中 4 个有向图彼此不同构.

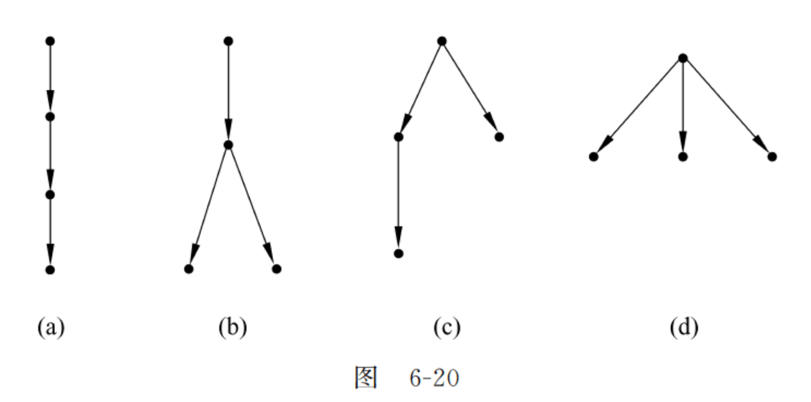


图 6-20

7. 若一个简单无向图 G 与其补图 $\overline{G}$ 同构，则称 G 为**自补图**.

(1) 试画出所有不同构的 5 阶自补图.

(2) 若 G 是 n 阶自补图，则 K_n 的边数为偶数.

(3) 若 G 是 $n(n\geqslant 2)$ 阶自补图，则存在正整数 k 使得 $n=4k$ 或 $n=4k+1$.

(4) 是否存在 6 阶自补图？

8. 试就 $n=3$ 证明乌拉姆(Ulam)猜想.

6.4 路与回路

在图 $G=(V,E)$ 中，经常考虑从一个节点出发，沿着一些边连续移动到另一个节点的问题，这就是路的概念，它与七桥问题密切相关.

6.4.1 路

【定义 6-13】 在任意一个图 $G=(V,E)$ 中，称 G 中节点与边交替出现的序列 L：$v_0e_1v_1e_2v_2\cdots v_{i-1}e_iv_i\cdots e_lv_l$ 为从 v_0 到 v_l 一条**路**(walk, way)，其中对于 $i=1,2,\cdots,l$，v_{i-1} 是 e_i 的起点，v_i 是 e_i 的终点.

在从 v_0 到 v_l 路 L：$v_0e_1v_1e_2v_2\cdots v_{i-1}e_iv_i\cdots e_lv_l$ 中，v_0 称为路的起点，v_l 称为路的终点，L 所经过的边数 l 称为**路的长度**(length of walk)或**跳数**(hop number). 特别地，单独一个节点 v 构成的序列是 v 到 v 的长度为 0 的路，称为**平凡路**.

例如，在图 6-21(a)中 $v_3e_3v_2e_2v_2e_3v_3e_4v_1$ 是一条从 v_3 到 v_1 长度为 4 的路，在图 6-21(b)中 $v_1e_7v_1e_1v_2e_3v_3$ 是一条从 v_1 到 v_3 长度为 3 的路. 需要注意的是，有向图中的路须按边的方向走，有向图中的路可称为有向路.

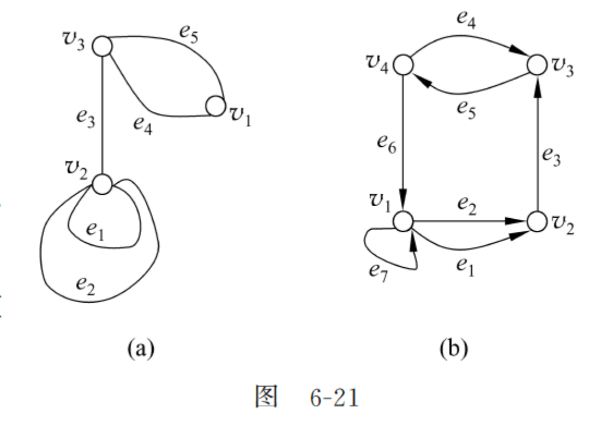


图 6-21

在不引起混淆的情况下，可以将路 L：$v_0e_1v_1e_2v_2\cdots v_{i-1}e_iv_i\cdots e_lv_l$ 简记为 L：$v_0v_1v_2\cdots v_{i-1}v_i\cdots v_l$ 或 L：$e_1e_2\cdots e_i\cdots e_l$.

在路中，有两种特殊的路. 一种是节点不重复的路，称为**路径**(path). 一种是边不重复的路，称为**轨迹**(trail).

显然，路径是轨迹，但轨迹不一定是路径. 如在图 6-21(a)中 $v_3e_3v_2e_2v_2$ 是一条从 v_3 到 v_2 的轨迹，但不是路径.

说明 由于图论应用的广泛性，很多概念存在意义上的差别. 之所以选择"路径"，它有捷径之意；"轨迹"强调边不重复，它是(可能多次)走过后留下的痕迹.

在 n 阶图 $G=(V,E)$ 中，若存在从节点 v_0 到另一个节点 v_l 的一条路，可将所有重复走的部分如 $v_i\cdots v_i$ 改为 v_i(去掉重复部分)，一直到没有节点重复为止，由于 n 阶图的任何路径的长度$\leqslant n-1$，于是存在一条从 v_0 到 v_l 一条长度$\leqslant n-1$ 的路径.

【定义 6-14】 在图 $G=(V,E)$ 中，称节点 u 到节点 v 的边数最少的长度为 u 到 v 的**距离**(distance)，记为 $d(u,v)$. 若节点 u 到 v 的路(径)不存在，则称 u 到 v 的距离为∞. 称 $\max\limits_{u,v\in V} d(u,v)$ 为图 G 的**直径**(diameter)，记为 $\mathrm{diam}(G)$.

显然，对于任意节点 $u,v\in V$ 有 $d(u,v)\geqslant 0$.

6.4.2 回路

【定义 6-15】 在图 $G=(V,E)$ 中，在路 L：$v_0e_1v_1e_2v_2\cdots v_{i-1}e_iv_i\cdots e_lv_l(l\geqslant 1)$ 中，起点 v_0 与终点 v_l 相同的路称为**回路**(circuit). 边不重复的回路称为**简单回路**(simple circuit)或**闭迹**(closed trail). 除起点重复一次外，别的节点均不重复的简单回路称为**圈或环**(cycle).

在图 6-22(a)中，1346527 是 G 的一条简单回路，这里用数字表示边，$abdeca$ 是 G 的一圈. 由定义易知，圈是简单回路，而简单回路不必是圈.

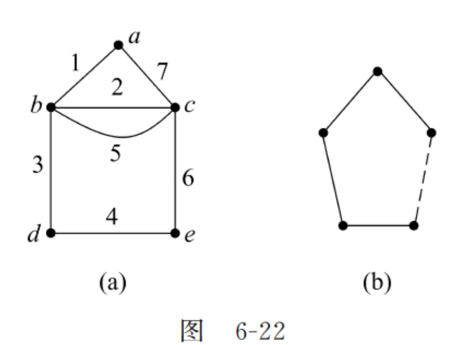


图 6-22

图论中的圈有圆圈之意，在计算机科学中常称为环，它有环路、循环的意思，但不要与是边的自环(loop)混淆了，因为自环是边，一般的环(cycle)是路.

圈的一般形式如图 6-22(b)所示，有 n 个节点的圈称为 **n 阶圈**，记为 C_n. 在 $n-1$ 阶圈 C_{n-1} 的内部放置一个节点，并使之与 C_{n-1} 的每个节点邻接，这样得到的图称为 **n 阶轮图**，记为 W_n.

由定义知，长度为 0 的路不称为回路. 显然，节点 v 到 v 的边可得到一个长度为 1 的圈.

类似地，在 n 阶图 $G=(V,E)$ 中，若存在从节点 v_0 到 v_0 的一条简单回路，则存在一条从 v_0 到 v_0 长度 $\leqslant n$ 的圈.

下面的定理很有用. 其证明过程用到了"最长路径法"技巧.

【定理 6-3】 在无向图 $G=(V,E)$ 中，若任意 $v\in V$ 有 $\deg(v)\geqslant 2$，则 G 中存在圈 .

证 不妨设 G 是简单图. 在 G 中选取一条最长的路径 L：$v_0v_1v_2\cdots v_l$，由于 L 是最长路径，与 v_0 邻接的节点必在 L 上. 设 $v_i(2\leqslant i\leqslant l)$ 与 v_0 邻接，则 $v_0v_1v_2\cdots v_iv_0$ 是 G 中的一个圈.

习 题 6.4

1. 在图 6-23(a)和图 6-23(b)中，分别找出一条包含所有边的轨迹.

2. 对于完全无向图 K_n，

(1) 共有多少个圈?

(2) 包含某条边的圈有多少个?

(3) 任意两个不同节点之间有多少条路径?

3. 在图 6-24 中，求节点 A 到节点 F 的：

(1) 所有路径；

(2) 所有轨迹；

(3) 距离.

4. 在图 6-25 中，求

(1) v_1 到 v_4 长度分别为 1,2,3 的路分别是哪些?

(2) v_1 到 v_1 长度分别为 1,2,3 的回路分别是哪些?

(3) 图 6-25 中长度为 3 的路共有多少条? 其中有多少条回路?

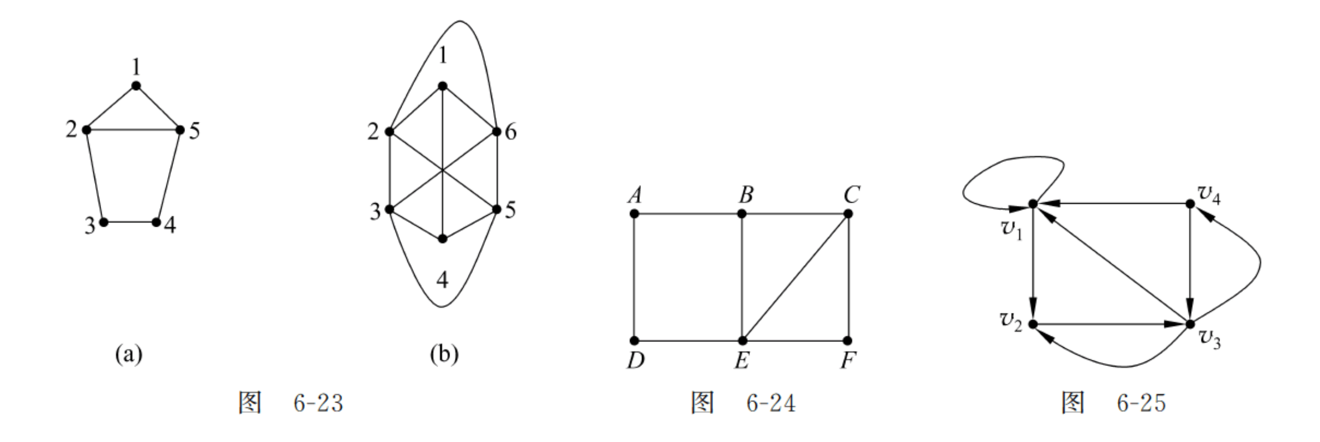


图 6-23　　图 6-24　　图 6-25

5. 若无向图 G 的任意两个节点之间都存在一条路，则 G 中任意两条最长轨迹存在公共节点.

6. 设 G 是简单有向图且 $k=\max\{\delta^+(G),\delta^-(G)\}$，则 G 中存在长度至少为 k 的轨迹.

7. 证明：在一个没有回路的竞赛图 G 中，对于任意节点 u 和 v 有

$$\mathrm{od}(u)\neq\mathrm{od}(v)$$

8. 若在有向图 $G=(V,E)$ 中，任意节点 $v\in V$ 的入度 $\mathrm{id}(v)\geqslant 2$，则 G 中至少含有两个不同的圈.

6.5 图的连通性

图的基本性质之一是其连通性，它与图中从节点到节点的路又是密切相关的. 为了讨论方便，先给出：

【定义 6-16】 在任何图 $G=(V,E)$ 中，若从节点 u 到 v 存在一条路，则称 u **可达** v(accessible).

由于节点 v 到 v 总存在一条长度为 0 的路，因此任意节点 v 可达 v 自身.

先讨论无向图的连通性.

6.5.1 无向图的连通性

【定义 6-17】 设 $G=(V,E)$ 是无向图，对于任意 $u,v\in V$ 均可达，则称 G 是**连通图**(connected graph).

显然，图 6-26(a)是连通图，而图 6-26(b)是非连通图.

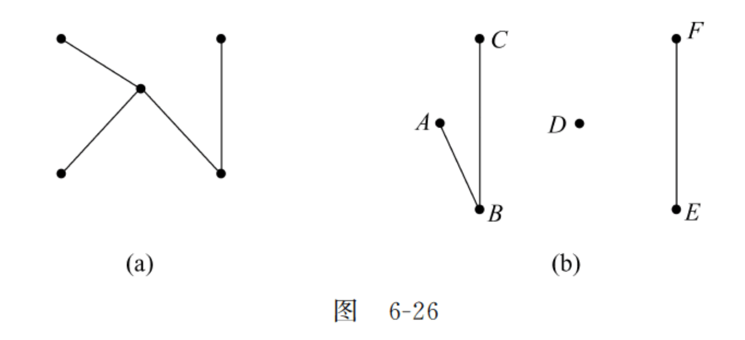


图 6-26

特别地,单独一个节点 v 是连通图,因为 v 到 v 存在长度为 0 的路,即 v 总是可达 v 的.

实际上,在任意无向图 $G=(V,E)$中有:

【定义 6-18】 设 $G=(V,E)$是无向图,G 中极大的连通子图称为 G 的**连通分支**(connected component),图 G 的连通分支数记为 $w(G)$.

由定义知,图 G 的连通分支满足 3 个条件:(1)连通分支是 G 的子图;(2)该子图本身是连通图;(3)在该子图中再添加原图 G 的任意边或节点都不连通.

在图 6-26(a)中图仅一个连通分支. 在图 6-26(b)中图有 3 个连通分支,它们分别是 $G[A,B,C]$,$G[D]$和 $G[E,F]$.

一个显然的结论如下:

【定理 6-4】 设 $G=(V,E)$是无向图,则 G 是连通图当且仅当 $w(G)=1$.

与定理 6-4 等价的命题是:无向图 G 非连通当且仅当 $w(G)\geqslant 2$.

【例 6-5】 设 $G=(V,E)$是简单无向图,若 G 不连通,则 G 的补图$\overline{G}$ 连通.

证 设 u 和 v 是$\overline{G}$ 中的任意两个节点.

(1) 若 u 和 v 在 G 中不邻接,则根据补图的定义知,u 和 v 在$\overline{G}$ 中邻接,于是 u 可达 v.

(2) 若 u 和 v 在 G 中邻接,则 u 和 v 必在图 G 的同一个连通分支 C_1 中. 由于 G 不连通,$w(G)\geqslant 2$. 设 C_2 是 G 的另一个连通分支,在 C_2 中选取节点 w,则在 G 中 u 和 w 在 G 中不邻接且 v 和 w 在 G 中不邻接,于是 u 和 w 在$\overline{G}$ 中邻接且 v 和 w 在$\overline{G}$ 中邻接,进而 uwv 是$\overline{G}$ 中从 u 到 v 的一条路,于是 u 可达 v.

由(1)和(2)知,$\overline{G}$ 是连通图.

【例 6-6】 设 $G=(V,E)$是 n 阶简单无向图,若对于任意的 G 中不相邻的节点 u 和 v 有 $\deg(u)+\deg(v)\geqslant n-1$,则 G 是连通图.

证 (反证法) 设 G 不连通,则 G 至少有两个连通分支 C_1 和 C_2,设其节点数分别为 n_1 和 n_2. 显然,$n_1+n_2\leqslant n$. 在 C_1 中取节点 u,在 C_2 中取节点 v,这时 u 和 v 在 G 中不相邻且 $\deg(u)\leqslant n_1-1$ 及 $\deg(v)\leqslant n_2-1$,于是

$$\deg(u)+\deg(v)\leqslant(n_1-1)+(n_2-1)\leqslant n-2<n-1$$

与已知矛盾.

注意 *在离散问题讨论中,经常使用反证法.*

上面的两个例子给出了证明无向图连通常用方法. 下面的结论也是很有用的.

【定理 6-5】 设 $G=(V,E)$是连通无向图,则

(1) 去掉 G 中任意简单回路 C 上的一条边 e 得到的图 $G-e$ 连通.

(2) 去掉度数为 1 的节点 v 得到的图 $G-v$ 连通.

证 (留作练习).

6.5.2 无向连通图的点连通度与边连通度

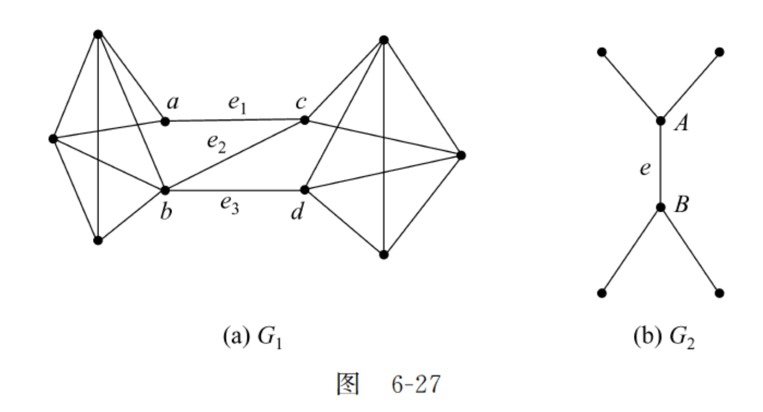
对于无向连通图,其连通的程度是不同的,有些很“脆弱”,有的则相反.

1. 点割集与点连通度$\kappa(G)$

【定义 6-19】 设 $G=(V,E)$是连通无向图且 $W\subset V$,若从 G 中删除 W 的所有节点所得到的子图不连通或是 1 阶图,而删除 W 的任意真子集都连通,则称 W 为 G 的**点割集**(cut-set of vertices).

“割”是分割、分离、分开的意思，恰使得 G 不连通或是 1 阶图所要去掉的节点集合称为 G 的点割集. 若点割集 $W=\{v\}$，则称 v 为 G 的**割点**(cut point)或**关节点**[21](articulation point).

由定义知，1 阶图的点割集为 $\varnothing$. 在图 6-27(a)中，$\{a,b\}$ 和 $\{c,d\}$ 是 G_1 的点割集，在图 6-27(b)中，A 和 B 是 G_2 的割点.



(a) G_1　　(b) G_2

图　6-27

【定义 6-20】　设 $G=(V,E)$ 是连通无向图，称 $\min\{|W|;W$ 是 G 的点割集$\}$ 为 G 的**点连通度**(vertex-connectivity)，简称**连通度**，记为 $\kappa(G)$.

根据定义，一个连通无向图 G 的点连通度是使得 G 不连通或为 1 阶图所要删去的最少的节点个数. 于是，1 阶图的点连通度为 0，而完全无向图 K_n 的点连通度 $\kappa(K_n)=n-1$.

在图 6-27(a)中图 G_1 的点连通度为 2，在图 6-27(b)中图 G_2 的点连通度为 1.

点连通度 $\kappa(G)=2$ 的图称为 2-连通或**重连通图**(biconnected graph). 确定一个无向图是否重连通具有重要的意义. 假定无向图的节点表示电话交换站，边表示电话线，则在点连通度为 2 的通信网络系统中，一个站发生故障系统仍可正常工作.

2. 边割集与边连通度 $\lambda(G)$

【定义 6-21】　设 $G=(V,E)$ 是连通无向图且 $F\subset E$，若从 G 中删除 F 的所有边所得到的子图不连通或是平凡图，而删除 F 的任意真子集都连通，则称 F 为 G 的**边割集**(cut-set of edges).

恰使得 G 不连通或是平凡图所要去掉的边的集合称为 G 的边割集. 若边割集 $F=\{e\}$，则称 e 为 G 的**割边**或**桥**(bridge).

在图 6-27(a)中，$\{e_1,e_2,e_3\}$ 是 G_1 的边割集，在图 6-27(b)中，e 是 G_2 的割边(或桥).

【定义 6-22】　设 $G=(V,E)$ 是连通无向图，称 $\min\{|F|;F$ 是 G 的边割集$\}$ 为 G 的**边连通度**(edge-connectivity)，记为 $\lambda(G)$.

根据定义，一个连通无向图 G 的边连通度是使得 G 不连通或为平凡图所要删去的最少的边的数目.

在图 6-27(a)中图 G_1 的边连通度为 3，在图 6-27(b)中图 G_2 的边连通度为 1.

下面的定理是 H. Whitney 在 1932 年给出的关于点连通度、边连通度及最小度之间的联系的一个结论.

【定理 6-6】　设 $G=(V,E)$ 是连通无向图，则 $\kappa(G)\leqslant\lambda(G)\leqslant\delta(G)$.

证　(1) 先证 $\lambda(G)\leqslant\delta(G)$. 由于将任意一个节点所关联的边全去掉后都不连通，所以有 $\lambda(G)\leqslant\delta(G)$.

(2) 再证 $\kappa(G)\leqslant\lambda(G)$. 当 $\lambda(G)=0$ 或 1 时,结论显然成立. 下设 $\lambda(G)\geqslant 2$. 于是,在 G 中删除含边割集的 $\lambda(G)$ 条边后得到的图不连通,而删除其中的 $\lambda(G)-1$ 条边仍连通但有一条桥 uv. 对于删除的 $\lambda(G)-1$ 的每一条边都选取一个不同于 u 和 v 的端点,当把这些端点都去掉时至少删除了 $\lambda(G)-1$ 条边. 若这样得到的图不连通,则 $\kappa(G)\leqslant\lambda(G)-1<\lambda(G)$. 若这样得到的图连通,则由于 uv 是桥,此时再删除 u 和 v 中的一个端点,所得到的图必不连通或是 1 阶图,此时 $\kappa(G)\leqslant\lambda(G)$. 所以,有 $\kappa(G)\leqslant\lambda(G)$ 成立.

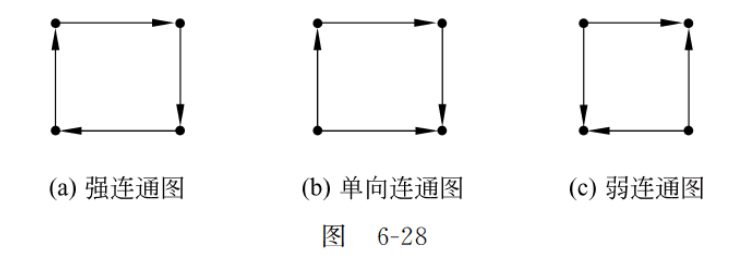
6.5.3 有向图的连通性

无向图只有连通与不连通两种情况,而有向图存在多种连通特性. 有向图的连通性分下述 3 种情形分别讨论.

1. 强连通图

【定义 6-23】 设 $G=(V,E)$ 是有向图,对于任意 $u,v\in V$,u 和 v 相互可达,则称 G 为**强连通图**(strongly connected digraph).

由定义易知,如图 6-28(a)所示是一个强连通图. 特别地,1 阶图是强连通图.



(a) 强连通图　(b) 单向连通图　(c) 弱连通图

图 6-28

【定理 6-7】 设 $G=(V,E)$ 是 n 阶($n\geqslant 2$)有向图,则 G 强连通当且仅当 G 中存在一条回路,它通过所有节点.

证 (⇒)设 G 的节点为 $v_1,v_2,\cdots,v_{n-1},v_n$. 由于 G 是强连通图,G 中任意两个节点相互可达,于是 v_1 到 v_2,v_2 到 v_3,$\cdots$,v_{n-1} 到 v_n,v_n 到 v_1 存在路,因此存在一条回路通过所有节点.

(⇐)显然.

【定义 6-24】 设 $G=(V,E)$ 是有向图,G 的极大的强连通子图称为 G 的**强连通分支**(strongly connected component).

由定义知,如图 6-29 所示有 4 个强连通分支,分别是 $G[1,2,3]$,$G[4]$,$G[5]$和 $G[6]$.

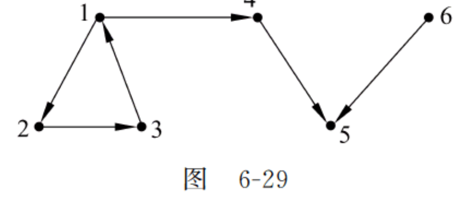


图 6-29

【定理 6-8】 设 $G=(V,E)$ 是有向图,则 G 的任意节点 $v\in V$ 都位于且仅位于 G 的一个强连通分支中.

证 对于任意 $v\in V$,令 W 是 G 的所有与 v 相互都存在路的节点组成的集合,则 $G[W]$是 G 的一个强连通分支且 v 位于 $G[W]$中.

若节点 v 位于两个不同的强连通分支 C_1 和 C_2 中,则任意的 C_1 和 C_2 中的节点都相互有路,于是得到一个更大的强连通子图,矛盾.

2. 单向连通图

【定义 6-25】 设 $G=(V,E)$ 是有向图,对于任意 $u,v\in V$,从 u 可达 v 或者从 v 可达 u,则称 G 为**单向连通图**(unilateral connected digraph).

由定义易知,如图 6-28(b)所示是一个单向连通图.

与定理 6-7 一样，下述定理对确定有向图的单向连通分支是非常有用的.

【定理 6-9】 设 $G=(V,E)$是有向图，则 G 单向连通当且仅当 G 中存在一条路，它通过所有节点 .

证 （$\Rightarrow$）若能证明命题"对于任意 $W\subseteq V$ 均存在一个 W 中节点在 G 中到 W 中其余节点都有路"，则定理结论成立. 因为先取 $W=V$，存在 $v_1\in W$ 到其余 V 中节点有路. 再取 $W=V-\{v_1\}$，存在 $v_2\in W$ 到其余 $V-\{v_1\}$ 节点有路. 这样一直下去，就可以得到一条从 v_1 到 v_2，v_2 到 v_3，…，v_{n-1} 到 v_n 的一条路，其中 $|V|=n$（但这条路不一定是轨迹）.

假定上述命题不成立. 令 $W=\{u_1,u_2,\cdots,u_{k-1},u_k\}$是使其不成立的元素个数最少的，这时 $k\geqslant 3$. 根据假设 $W-\{u_k\}$使命题成立，于是必存在 $W-\{u_k\}$中一个节点，不妨设为 u_1 到其余节点 $u_2,\cdots,u_{k-1}$有路，而假设 u_1 到 u_k 是没有路的，否则与 W 的假设矛盾. 另一方面，由于 u_1 到其余节点 $u_2,\cdots,u_{k-1}$有路，所以 u_k 到 u_1 没有路，否则 u_k 到 $u_1,u_2,\cdots,u_{k-1}$都有路. 由于 u_1 到 u_k 没有路，而 u_k 到 u_1 也没有路，与已知 G 是单向连通图矛盾.

（$\Leftarrow$）显然.

【定义 6-26】 设 $G=(V,E)$是有向图，G 的极大的单向连通子图称为 G 的**单向连通分支**（unilateral connected component）.

由定义知，如图 6-29 所示有两个单向连通分支，分别是 $G[1,2,3,4,5]$，$G[5,6]$.

注意 *有向图 G 的节点 $v\in V$ 可以位于 G 的不同的单向连通分支中.*

3. 弱连通图

【定义 6-27】 设 $G=(V,E)$是有向图，若 G 不考虑边的方向是一个无向连通图，则称有向图 G 为**弱连通图**（weakly connected digraph），简称有向图 G 连通.

由定义易知，如图 6-28(c)所示是一个弱连通图.

显然，强连通图是单向连通图且单向连通图是弱连通图，但反过来都不成立（参见如图 6-28 所示）.

最后给出下面的定义.

【定义 6-28】 设 $G=(V,E)$是有向图，G 的极大的弱连通子图称为 G 的**弱连通分支**（weakly connected component）.

习 题 6.5

1. 设 $G=(V,E)$是连通无向图，则

（1）去掉 G 中任意简单回路 C 上的一条边 e 得到的图 $G-e$ 连通.

（2）去掉度数为 1 的节点 v 得到的图 $G-v$ 连通.

2. 设 G 是 $n(n\geqslant 2)$阶简单无向图，若 $\delta(G)\geqslant n/2$，则 G 是连通图.

3. 设 G 是(n,m)简单图且 $n\geqslant 3$，若 $m>C_{n-1}^2$，则 G 是连通图.

4. 对于简单连通无向图 $G=(V,E)$，若 G 不是完全图，则存在 3 个节点 $u,v,w\in V$ 使得$\{u,v\}\in E$ 且$\{v,w\}\in E$ 但$\{u,w\}\notin E$.

5. 设 $G=(V,E)$是简单连通无向图，$\delta(G)=k\geqslant 1$，

（1）若 G 中最长的路径的长度为 l，则 $l\geqslant k$.

（2）对于任意的 G 中最长的路径为 $v_0v_1\cdots v_l$，$G-\{v_0,v_1,\cdots,v_{k-1}\}$是连通图.

(3) 举例说明,对于 G 中最长的轨迹,(2)中结论不成立.

6. 证明:无向图 G 中节点之间的可达关系 P 是一个等价关系,并说明其等价类是什么?

7. 分别求出 n 阶完全无向图 K_n 的点连通度和边连通度.

8. 设 G 是 n 阶简单连通无向图,若 $n>2\delta(G)$,则 G 存在一条长至少为 $2\delta(G)$ 的路径.

9. 设 G 是 $n(n\geqslant 2)$ 阶无向图,若 $\delta(G)\geqslant(n+k-1)/2(1\leqslant k\leqslant n-1)$,则 $\kappa(G)\geqslant k$.

10. 设 G 是 (n,m) 简单连通无向图,则 $\lambda(G)\leqslant 2m/n$.

11. 求出图 6-30 所示的有向图 G 的所有强连通分支、单向连通分支和弱连通分支.

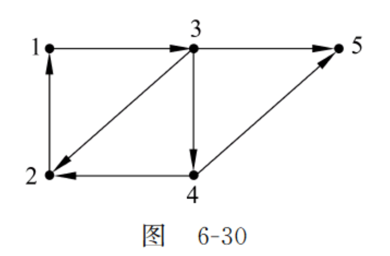


图 6-30

12. 设 $G=(V,E)$ 是非平凡有向图,若对于任意 $\varnothing\neq W\subset V$,$G$ 中起点在 W,终点在 $V-W$ 的边至少 k 条,则称有向图 G 的边连通度至少为 k. 证明:非平凡有向图 G 是强连通的充要条件是 G 的边连通度至少为 1.

6.6 图的矩阵表示

将一个图画出来是最直观的表示图的方式. 为了便于使用计算机存储和处理图,更为了借助于完善的矩阵理论研究图的有关性质,有必要学习图的矩阵表示.

本节简单介绍图的常见的 3 种矩阵表示及一些简单结论,不涉及更多的有关图的矩阵方面的知识[16, 18].

6.6.1 图的邻接矩阵

第一种图的矩阵表示——邻接矩阵,它表示的是图中任意两个节点间的邻接关系.

【定义 6-29】 设 $G=(V,E)$ 是图,节点集合已编号 $V=\{v_1,v_2,\cdots,v_n\}$,则 G 的**邻接矩阵**(adjacency matrix)$\mathbf{A}(G)=(a_{ij})_{n\times n}$ 中元素 a_{ij} 是 v_i 邻接到 v_j 的边数 $(i,j=1,2,\cdots,n)$.

在图 6-31(a)和图 6-31(b)中,图 G_1 和 G_2 的邻接矩阵分别为:

$$\mathbf{A}(G_1)=\begin{bmatrix}0&2&1&0\\2&0&0&1\\1&0&1&1\\0&1&1&0\end{bmatrix},\quad \mathbf{A}(G_2)=\begin{bmatrix}0&2&0&0\\0&0&0&1\\1&0&1&0\\0&0&1&0\end{bmatrix}$$

显然,无向图的邻接矩阵是对称矩阵且一个图与其邻接矩阵是一一对应的.

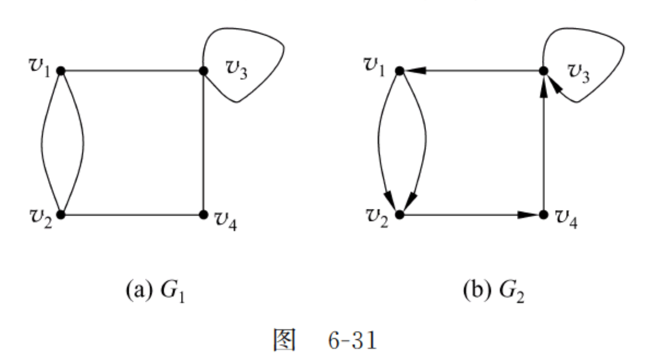


图 6-31

从一个图的邻接矩阵容易得出每个节点的度数，以有向图 G 为例，$\boldsymbol{A}(G)$ 中第 i 行元素之和为第 i 个节点 v_i 的出度($i=1,2,\cdots,n$)，第 j 列元素之和为第 j 个节点 v_j 的入度($j=1,2,\cdots,n$).

从图的邻接矩阵可以得出从节点 v_i 到 v_j 长度为 $l(l\geqslant 1)$ 的路的数目.

【定理 6-10】 设 $\boldsymbol{A}$ 是图 G 的邻接矩阵，则 $\boldsymbol{A}^l(l\geqslant 1)$ 中 (i,j) 位置元素 $a_{ij}^{(l)}$ 为从节点 v_i 到 v_j 长度为 l 的路的数目.

证 设 G 是 n 阶图. 对 l 使用数学归纳法. 当 $l=1$ 时，结论成立.

假设 $l-1$ 时成立，考虑 $\boldsymbol{A}^l$ 中 (i,j) 位置元素 $a_{ij}^{(l)}$. 根据矩阵乘法知，由于 $a_{ij}^{(l)}=\sum_{k=1}^{n}a_{ik}^{(l-1)}\cdot a_{kj}$，所以 $a_{ik}^{(l-1)}a_{kj}$ 表示从 v_i 到 v_k 长度为 $l-1$ 再从 v_k 到 v_j 长度为 1 的路的数目($k=1,2,\cdots,n$)，进而 $a_{ij}^{(l)}=\sum_{k=1}^{n}a_{ik}^{(l-1)}\cdot a_{kj}$ 是 v_i 到 v_j 长度为 l 的路的数目.

注意 在离散问题讨论中，数学归纳法也是经常使用的一种证明方法.

【例 6-7】 在如图 6-32 所示的有向图 G 中，

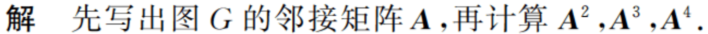
(1) 求出从 v_2 到 v_5 长度为 1,2,3,4 的路各有多少条？

(2) G 中长度为 3 的路共有多少条？其中有多少条是回路？

(3) G 是哪类连通图？

图 6-32

解 先写出图 G 的邻接矩阵 $\boldsymbol{A}$，再计算 $\boldsymbol{A}^2,\boldsymbol{A}^3,\boldsymbol{A}^4$.



$$\boldsymbol{A}=\begin{bmatrix}0&1&0&1&0\\0&0&0&0&1\\0&1&0&1&0\\0&0&0&0&1\\1&0&1&0&0\end{bmatrix},\quad \boldsymbol{A}^2=\boldsymbol{A}\cdot\boldsymbol{A}=\begin{bmatrix}0&0&0&0&2\\1&0&1&0&0\\0&0&0&0&2\\1&0&1&0&0\\0&2&0&2&0\end{bmatrix},$$

$$\boldsymbol{A}^3=\boldsymbol{A}^2\cdot\boldsymbol{A}=\begin{bmatrix}2&0&2&0&0\\0&2&0&2&0\\2&0&2&0&0\\0&2&0&2&0\\0&0&0&0&4\end{bmatrix},\quad \boldsymbol{A}^4=\boldsymbol{A}^3\cdot\boldsymbol{A}=\begin{bmatrix}0&4&0&4&0\\0&0&0&0&4\\0&4&0&4&0\\0&0&0&0&4\\4&0&4&0&0\end{bmatrix}.$$

(1) 从 v_2 到 v_5 长度为 1,2,3,4 的路分别有 1，0，0，4 条.

(2) 由于 $\boldsymbol{A}^3$ 中所有元素之和为 20，所以 G 中长度为 3 的路共有 20 条. 又由于对角线上元素之和为 12，故其中有 12 条是回路.

(3) 从 $\boldsymbol{A},\boldsymbol{A}^2,\boldsymbol{A}^3,\boldsymbol{A}^4$ 知，均有 (i,j) 位置元素不为 0 的情况，说明 G 中任意两个节点之间均相互存在路，所以 G 是强连通图.

6.6.2 图的可达矩阵

第二种图的矩阵表示——可达矩阵，它表示的是图中任意两个节点间的可达关系.

【定义 6-30】 设 $G=(V,E)$ 是图，节点集合已编号 $V=\{v_1,v_2,\cdots,v_n\}$，则 G 的**可达矩阵**(accessible matrix)$\boldsymbol{P}(G)=(p_{ij})_{n\times n}$ 中元素 p_{ij} 如下选取

$$p_{ij}=\begin{cases}1, & v_i \text{ 可达 } v_j\\0, & \text{其他}\end{cases},\quad i,j=1,2,\cdots,n$$

例 6-7 中图的可达矩阵为

$$P(G)=\begin{bmatrix}1&1&1&1&1\\1&1&1&1&1\\1&1&1&1&1\\1&1&1&1&1\\1&1&1&1&1\end{bmatrix}$$

容易由图的邻接矩阵 $\boldsymbol{A}(G)$得出其可达矩阵 $\boldsymbol{P}(G)$,一个非常有效的算法是 Warshall 算法[8,9].根据我们的可达矩阵的定义知,$\boldsymbol{P}(G)$中所有主对角线上的元素全为 1,这是由于任意节点可达自身所致.

更容易从图的可达矩阵得出图的连通性质.

6.6.3　图的关联矩阵

第三种图的矩阵表示——关联矩阵,它表示的是图中节点与边之间的关联关系.

1. 无向图

【定义 6-31】 设 $G=(V,E)$是无向图,节点集合和边集合均已编号 $V=\{v_1,v_2,\cdots,v_n\}$,$E=\{e_1,e_2,\cdots,e_m\}$,则 G 的**关联矩阵**(incidence matrix)$\boldsymbol{M}(G)=(m_{ij})_{n\times m}$中元素 m_{ij} 为节点 v_i 与边 e_j 的关联次数.

【例 6-8】 求出如图 6-33(a)所示中无向图 G_1 的关联矩阵.

解　G_1 的关联矩阵为 $\boldsymbol{M}(G_1)=\begin{bmatrix}2&0&0&1&0\\0&1&1&0&0\\0&1&1&0&1\\0&0&0&1&1\end{bmatrix}$.

根据图的关联矩阵可得到图的一些性质,如节点的度数、是否存在多重边、是否存在孤立点等.

2. 有向图

【定义 6-32】 设 $G=(V,E)$是无自环(loop)的有向图,节点集合和边集合均已编号 $V=\{v_1,v_2,\cdots,v_n\}$,$E=\{e_1,e_2,\cdots,e_m\}$,则 G 的**关联矩阵**(incidence matrix)$\boldsymbol{M}(G)=(m_{ij})_{n\times m}$中元素 m_{ij} 为

$$m_{ij}=\begin{cases}1, & v_i \text{ 为 } e_j \text{ 的起点}\\ -1, & v_i \text{ 为 } e_j \text{ 的终点},\quad i=1,2,\cdots,n;j=1,2,\cdots,m.\\ 0, & v_i \text{ 与 } e_j \text{ 不关联}\end{cases}$$

【例 6-9】 求出如图 6-33(b)所示中有向图 G_2 的关联矩阵.

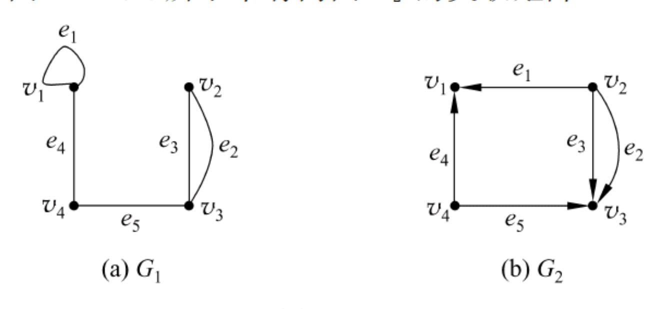


图　6-33

解　G_2 的关联矩阵为 $\boldsymbol{M}(G_2)=\begin{bmatrix} -1 & 0 & 0 & -1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & -1 & -1 & 0 & -1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$.

图还有其他矩阵表示，如距离矩阵、圈矩阵以及割集矩阵等，参考有关文献[16～19]. 前面已经谈到，有了这些图的矩阵表示，可以用线性代数中的知识，特别是矩阵理论对图做更深入的研究，由于篇幅所限，本书不涉及这些内容的进一步讨论，可参见有关图论文献.

习　题　6.6

1. 分别写出如图 6-34(a)和图 6-34(b)所示的邻接矩阵和可达矩阵.

2. 图 6-35 所示的是一个有向图 G.

(1) 求出从 v_3 到 v_2 长度为 4 的路各有多少条？并从图中列举出来.

(2) G 中长度为 3 的路共有多少条？其中有多少条是回路？

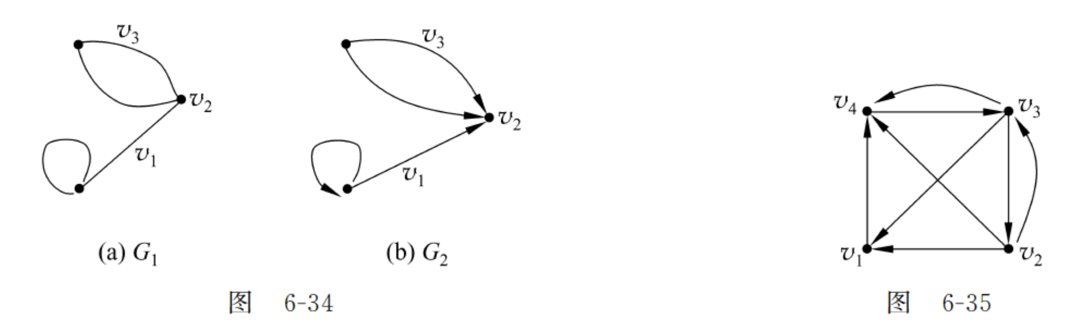


图　6-34　　　　图　6-35

(3) G 是哪类连通图？

3. 在如图 6-36 所示的有向图 G 中，

(1) 计算图 G 的邻接矩阵 $\boldsymbol{A}$.

(2) G 中 v_1 到 v_4 的长度为 4 的路有多少条，并根据图分别表示出来.

(3) G 中 v_1 到 v_1 的长度为 3 的回路有多少条，并根据图表示出来.

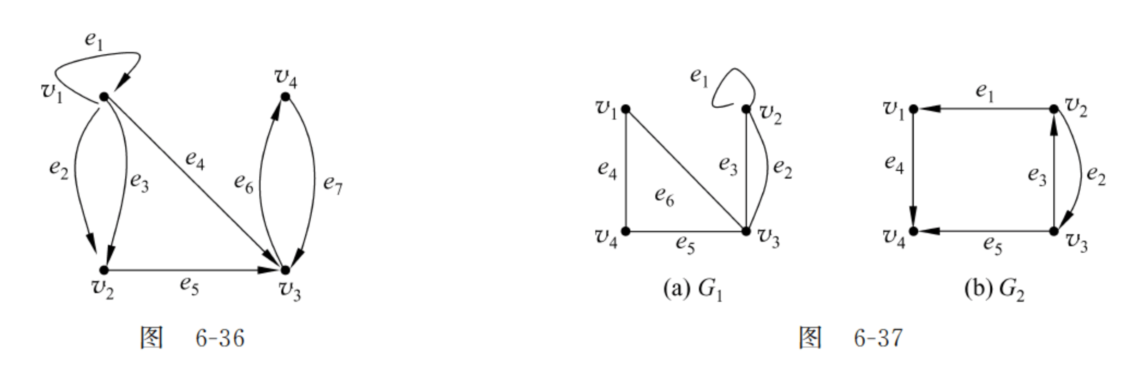


图　6-36　　　　图　6-37

(4) G 中长度为 4 的路共有多少条？其中有多少条是回路？

(5) G 中长度≤4 的路共有多少条？其中有多少条是回路？

(6) G 是哪类连通图？

4. 求出图 6-37 所示的无向图 G_1 及有向图 G_2 的关联矩阵.

5. 给定图 $G=(V,E)$，其中 $V=\{v_1,v_2,\cdots,v_n\}$，定义 G 的**距离矩阵**为 $\boldsymbol{D}=(d_{ij})_{n\times n}$，其中 $d_{ij}=d(v_i,v_j)$，$i,j=1,2,\cdots,n$. 试写出如图 6-38 所示中图 G 的距离矩阵 $\boldsymbol{D}(G)$.

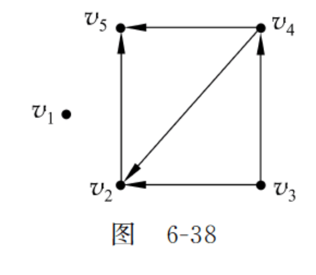


图 6-38

6. 已知有向图 G 的邻接矩阵为 $\boldsymbol{A}=\begin{bmatrix}0&2&1&0\\0&0&1&0\\0&0&1&1\\0&0&0&1\end{bmatrix}$，画出图 G 的图形.

7. 已知无向图 G 的关联矩阵为 $\boldsymbol{M}=\begin{bmatrix}1&1&0&0&1&1\\1&1&1&0&0&0\\0&0&1&1&0&1\\0&0&0&1&1&0\\0&0&0&0&0&0\end{bmatrix}$，画出图 G 的图形.

6.7 赋权图及最短路径

6.7.1 赋权图

在图的实际应用中，除建立图论模型外，有时还需要将一些附加信息赋予图的边或节点，这就是**赋权图**(weighted graph). 本节仅讨论边赋权图.

【定义 6-33】 设 $G=(V,E)$ 是任意图，若 G 的每一条边上都赋予一个非负实数，则称 G 是**边赋权图**.

如图 6-39 所示是两个边赋权图.

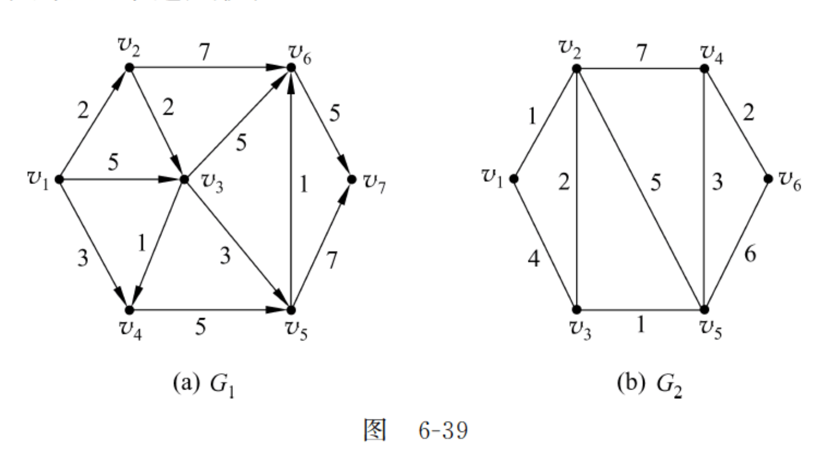


图 6-39

在边赋权图 $G=(V,E)$ 中，每条边上所赋的非负实数称为这条边上的权，它可以理解为该边上的流量或通过该边的时间、费用，还可以理解为该边的长度.

赋权图 6-39 的邻接矩阵分别为

$$A(G_1)=\begin{pmatrix}0&2&5&3&0&0&0\\0&0&2&0&0&7&0\\0&0&0&1&3&5&0\\0&0&0&0&5&0&0\\0&0&0&0&0&1&7\\0&0&0&0&0&0&5\\0&0&0&0&0&0&0\end{pmatrix},\quad A(G_2)=\begin{pmatrix}0&1&4&0&0&0\\1&0&2&7&5&0\\4&2&0&0&1&0\\0&7&0&0&3&2\\0&5&1&3&0&6\\0&0&0&2&6&0\end{pmatrix}$$

6.7.2 最短路径

在边赋权图 $G=(V,E)$ 中，从一个节点到另一个节点的路上所有边上的权之和称为该路的“权”，例如在图 6-39(a)中路 $v_2v_3v_5v_6v_7$ 的权为 $2+3+1+5=11$.

在实际应用中，最短线路的铺设、运输网络的最少时间以及互联网上的最短路由问题等，都需要得出从一个节点到别的节点权最小的一条路，它必为路径，称为**最短路径**.

荷兰著名计算机专家 E. W. Dijkstra 于 1959 年提出的求一个节点到其他任意节点的最短路径算法，是至今为止被大家公认的有效算法，其时间复杂度为 $O(n^2)$，其中 n 为图的节点个数.

设 $G=(V,E)$ 是 n 阶边赋权图，$V=\{v_1,v_2,\cdots,v_n\}$，用 w_{ij} 表示节点 v_i 到 v_j 的边上的权 $(i.j=1,2,\cdots,n)$，若 v_i 到 v_j 无边，则令 $w_{ij}=+\infty$.

目标：求节点 v_1 到其他任意节点的最短路径.

Dijkstra(迪杰斯特拉) 算法将 V 划分成两部分 P 和 T，P 表示永久性节点集，而 $T=V-P$ 称为临时节点集. 对 P 的每节点 v 进行 P 标号 $l(v)$，表示节点 v_1 到 v 的最短路径的权，而 T 中每节点 v 的 T 标号 $l(v)$ 表示节点 v_1 到 v 的一条路上的权.

Dijkstra 算法：

(1) 令 $P=\{v_1\}$ 且 v_1 进行 P 标号 $l(v_1)=0$，对 $T=V-P$ 中节点进行 T 标号 $l(v_j)=w_{1j}$，$j=2,3,\cdots,n$.

(2) 在所有 T 标号的节点中，选取最小标号节点 v_i 进入 P.

(3) 重新按下列方式计算具有 T 标号的其他节点 v_j 的 T 标号：

$$\min\{l(v_j),l(v_i)+w_{ij}\}$$

(4) 重复上述(2)和(3)步骤，直至 $|P|=n$.

【例 6-10】 利用 Dijkstra 算法求出图 6-39 中从 v_1 到其余所有节点的最短路径.

解 以表格形式简化 Dijkstra 算法求解图 6-39(a)的过程如表 6-1 所示，其中 v_5 所在列 $\underline{7}/v_3$ 表示 v_3 在 v_1 到 v_5 的最短路径上，并且与 v_5 邻接，依此类推.

表 6-1

	v_1	v_2	v_3	v_4	v_5	v_6	v_7
1	$\underline{0}$	$\underline{2}/v_1$	5	3	∞	∞	∞
2			4	$\underline{3}/v_1$	∞	9	∞
3			$\underline{4}/v_2$		8	9	∞
4					$\underline{7}/v_3$	9	∞
5						$\underline{8}/v_5$	14
6							$\underline{13}/v_6$

于是,从 v_1 到其余各节点的最短路径如图 6-40(a)所示.

以表格形式简化 Dijkstra 算法求解图 6-39(b)的过程如表 6-2 所示.

表 6-2

	v_1	v_2	v_3	v_4	v_5	v_6
1	$\underline{0}$	$\underline{1}/v_1$	4	∞	∞	∞
2			$\underline{3}/v_2$	8	6	∞
3				8	$\underline{4}/v_3$	∞
4				$\underline{7}/v_5$		10
5						$\underline{9}/v_4$

于是,从 v_1 到其余各节点的最短路径如图 6-40(b)所示.

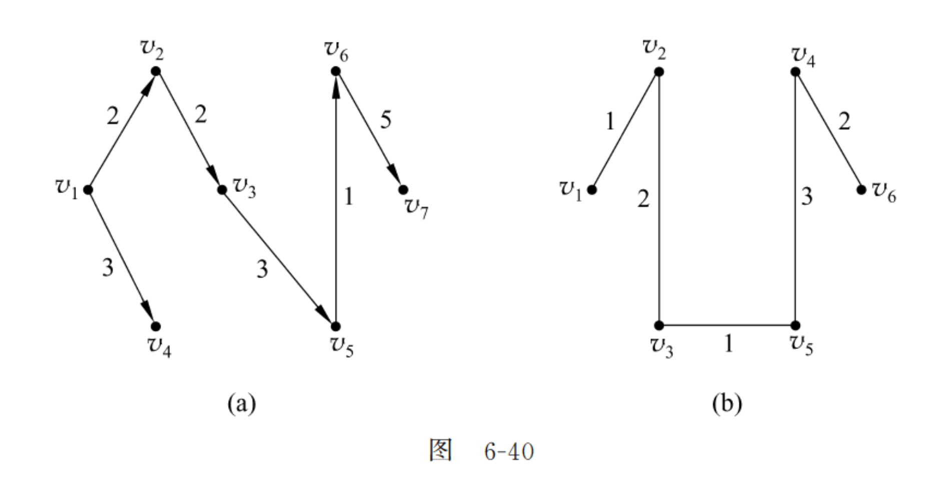


图 6-40

注意 Dijkstra 算法既适合于无向图,也适合于有向图.

下面介绍的 Warshall 算法是由 Warshall 给出并经 R. W. Floyd(弗洛伊德)改进的算法,它可求出任意两个点之间的最短路径,也可参见文献[13].

Warshall 算法:

(1) 令 $W^{(0)}=(w_{ij})=(w_{ij}^{(0)})$.

(2) 利用 $W^{(0)}$ 依次构造 $W^{(1)},W^{(2)},\cdots,W^{(n)}$,其中 $W^{(k)}=(w_{ij}^{(k)})$,$w_{ij}^{(k)}=\min\left\{w_{ij}^{(k-1)},w_{ik}^{(k-1)}+w_{kj}^{(k-1)}\right\}$,$w_{ij}^{(k)}$ 是从 v_i 到 v_j 中间节点仅属于 $\{v_1,v_2,\cdots,v_k\}$ 的最短路径的权.

最后得到的 $W^{(n)}$ 就是从 v_i 到 v_j 的最短路径的权.

与最短路径相反,需要考虑最长路径问题.在一个赋权图中,从一个(源)节点到另一个(汇)节点间的最长路径称为**关键路径**(critical path).

习 题 6.7

1. 在一个赋权图中,如何理解权为 0 边?对边上的权应怎样理解最好?
2. 在图 6-39(a)中,利用 Dijkstra 算法求出从 v_4 到其余各节点的最短路径.
3. 在赋权图 6-41 中,利用 Dijkstra 算法求出从 u 到 v 的所有最短路径及其权.

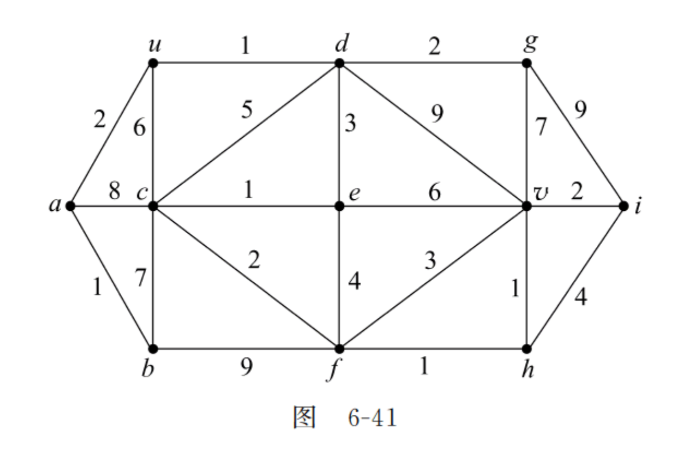


图　6-41

本章小结

1．图的基本概念

图 $G=(V,E)$主要由两部分组成：节点集合 V 和边集合 E. 通常研究有限的无向图和有向图.

设 $G=(V,E)$是图，节点 u 和 v 邻接是指从节点 u 到 v 有边. 在无向图 $G=(V,E)$中，两条边 e_1 和 e_2 邻接是指这两条边有公共端点. 设 $G=(V,E)$是图，边 e 与其两个端点是关联的.

无自环且无平行边的图是简单图，例如 K_n. 设 $G=(V,E)$是 n 阶简单无向图，由 G 的所有节点以及由能使 G 成为 K_n 需要添加的边构成的图为 G 的补图 $\overline{G}$.

深入理解图的定义，能对较简单的实际问题建立图模型.

2．节点的度数

设 $G=(V,E)$是无向图，与节点 v 关联的所有边数为节点 v 的度数 $\deg(v)$，节点处的一个自环算 2 度.

设 $G=(V,E)$是有向图，以 v 为起点的边的数目为节点 v 的出度 $\mathrm{od}(v)$，以 v 为终点的边的数目为节点 v 的入度 $\mathrm{id}(v)$，$\mathrm{od}(v)+\mathrm{id}(v)$是节点 v 的度数 $\deg(v)$.

握手定理　在任何(n,m)图 $G=(V,E)$中，其所有节点度数之和等于边数 m 的 2 倍，即

$$\sum_{v\in V}\deg(v)=2m.$$

掌握节点(出、入)度的定义，能熟练运用握手定理，了解孤立点、k-正则图、最大度 $\Delta(G)$、最小度 $\delta(G)$和度数序列等概念.

3．子图、图的运算和图同构

图 $G=(V,E)$的任意部分只要能构成图就是 G 的子图，产生子图的常见 4 种方式：$G[W]$，$G-W$，$G[F]$，$G-F$. 节点与 G 相同的子图是 G 的生成子图.

两个图同构 $G_1\cong G_2$ 是指这两个图本质上是同一个图.

理解子图的定义和两个图同构的直观含义，了解图的集合运算定义.

4．路与回路

在图 $G=(V,E)$中，从一个节点出发，沿着一些边连续移动到另一个节点就是路 L，L 所经过的边数称为路 L 的长度或跳数. 节点不重复的路称为路径；边不重复的路称为轨迹.

在图 $G=(V,E)$ 中，称节点 u 到节点 v 的边数最少的路径的长度为 u 到 v 的距离 $d(u,v)$. 图 G 的直径 $\operatorname{diam}(G)=\max\limits_{u,v\in V} d(u,v)$.

起点与终点相同的路称为回路. 边不重复的回路称为简单回路或闭迹. 除起点重复一次外，别的节点均不重复的简单回路称为圈或环.

掌握路、路的长度、路径、轨迹、距离、直径、回路、闭迹和圈的概念.

5. 图的连通性

(1) 无向图 $G=(V,E)$ 是连通图是指任意 $u,v\in V$ 均可达. 无向图 G 的连通分支是 G 的极大的连通子图. 能根据已知条件判断或证明图的连通性.

(2) 连通无向图 G 的点连通度 $\kappa(G)$ 是使得 G 不连通或为 1 阶图所要删去的最少的节点个数. 连通无向图 G 的边连通度 $\lambda(G)$ 是使得 G 不连通或为平凡图所要删去的最少的边的数目. 了解点连通度 $\kappa(G)$ 和边连通度 $\lambda(G)$.

(3) 有向图 $G=(V,E)$ 强连通图是指任意 $u,v\in V$，u 和 v 相互可达. 设 G 是 n ($n\geqslant 2$) 阶有向图，则 G 强连通当且仅当 G 中存在一条回路，它通过所有节点. 有向图 G 的极大的强连通子图称为 G 的强连通分支. 有向图 G 的任意节点 $v\in V$ 都位于且仅位于 G 的一个强连通分支中.

有向图 $G=(V,E)$ 单向连通图，是指对于任意 $u,v\in V$，从 u 可达 v 或者从 v 可达 u. 有向图 G 单向连通当且仅当 G 中存在一条路，它通过所有节点. 有向图 G 的极大的单向连通子图是 G 的单向连通分支.

有向图 G 弱连通图是指不考虑边的方向是无向连通图. 有向图 G 的极大的弱连通子图称为 G 的弱连通分支.

要求能判断有向图的连通性，求出有向图的强(单向、弱)连通分支.

6. 图的矩阵表示

设 $G=(V,E)$ 是图，节点集合编号 $V=\{v_1,v_2,\cdots,v_n\}$，则 G 的邻接矩阵 $\mathbf{A}(G)=(a_{ij})_{n\times n}$ 中元素 a_{ij} 是 v_i 邻接到 v_j 的边数($i,j=1,2,\cdots,n$).

定理 设 A 是图 G 的邻接矩阵，则 A^l ($l\geqslant 1$) 中 (i,j) 位置元素 $a_{ij}^{(l)}$ 为从节点 v_i 到 v_j 长度为 l 的路的数目.

掌握图邻接矩阵及上述结论，了解可达矩阵和关联矩阵.

7. 赋权图及最短路径

设 $G=(V,E)$ 是任意图，若 G 的每一条边上都赋予一个非负实数，则 G 是边赋权图.

两节点间权最小的一条路就是最短路径.

深入理解边赋权图，了解最短路径和求最短路径的 Dijkstra 算法.

第 7 章　几类特殊的图

图论是处理离散对象的一种重要的数学工具. 本章讨论几类在理论研究和实际应用中都有着重要意义的特殊图.

7.1　欧　拉　图

7.1.1　欧拉图的有关概念

欧拉图是 1736 年由年仅 29 岁的欧拉(Euler)研究“七桥问题”时考虑的一种图,由此得出 3 个概念.

【定义 7-1】　设 $G=(V,E)$是任意图,G 中经过所有边一次且仅一次的路称为**欧拉轨迹**(Eulerian trail)或**欧拉路**,G 中经过所有边一次且仅一次的回路称为**欧拉回路**(Eulerian circuit),存在欧拉回路的图称为**欧拉图**(Eulerian graph)或简称为 E 图.

显然,欧拉回路是欧拉轨迹,但反过来一般不成立. 如图 7-1(a)所示中的图存在欧拉轨迹,但不存在欧拉回路.

如图 7-1(b)所示中的图存在欧拉回路 $v_1v_2v_4v_1v_3v_2v_5v_3v_4v_5v_1$,它是欧拉图.

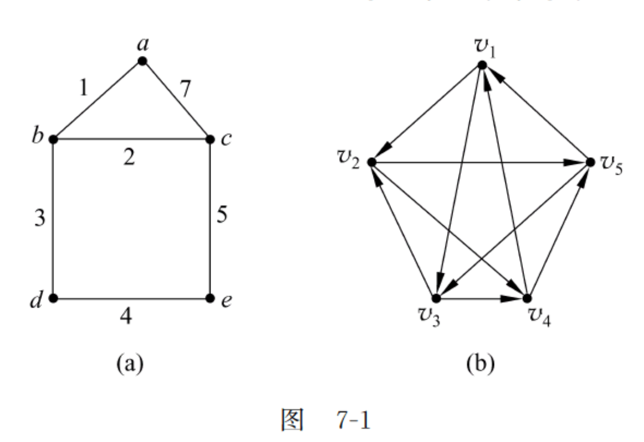


图　7-1

7.1.2　欧拉定理

【定理 7-1】　(**欧拉定理**)设 G 是非平凡连通无向图,则 G 是欧拉图的充要条件是 G 的每节点度数为偶数.

证　($\Rightarrow$)显然.

($\Leftarrow$)设 G 是(n,m)图. 若 $m=1$,则 G 是$(1,1)$图,结论成立. 假设对边数小于 m 的连通图结论成立,当边数为 m 时,由于 G 是非平凡连通图且每个节点度数为偶数,G 中每节点度数均$\geqslant 2$,由定理 6-3 知 G 中存在一个圈 C. 先从 G 中去掉 C 中的所有边得到一个图,其每一个连通分支的每节点度数为偶数,由归纳假设知,每一个连通分支是欧拉图,进而

存在欧拉回路，于是图 G 中通过回路 C 存在欧拉回路（如图 7-2 所示），故 G 是欧拉图.

欧拉定理给出了一个连通图存在欧拉回路的充要条件，但要具体找出一条这样的回路也是要有章可循的，随意行走是不行的，可参见图 7-2. 1921 年 Fleury 给出了一个求欧拉回路的算法[17].

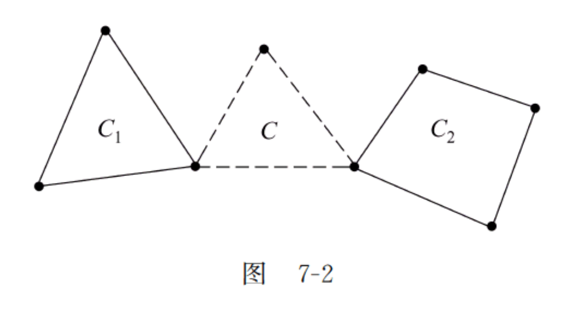


图 7-2

类似于欧拉定理有以下几个定理.

【定理 7-2】 设 G 是弱连通图，则 G 是欧拉图的充要条件是 G 的每节点的入度等于其出度.

【例 7-1】 设 G_1 和 G_2 是 n 阶完全图 $K_n(n\geqslant 4)$ 的两个不同的子图，若它们都是欧拉图，则 G_1 和 G_2 的环和 $G_1 \oplus G_2$ 的每个连通分支是欧拉图.

证 设 v 是 $G_1 \oplus G_2$ 中任意节点，根据已知条件及欧拉定理知，v 在 G_1 和 G_2 的度数 d_1 和 d_2 均为偶数. 若 v 在 $G_1 \cap G_2$ 的度数为 d，则 v 在 $G_1 \oplus G_2$ 中的度数为 d_1+d_2-2d 仍为偶数，所以 $G_1 \oplus G_2$ 的每个连通分支是欧拉图.

根据定理 7-1 容易得出以下定理.

【定理 7-3】 设 G 是连通无向图，则 G 中存在欧拉轨迹的充要条件是 G 的度数为奇数的节点个数为 0 或为 2.

证 若欧拉轨迹不是欧拉回路，只需在轨迹的起点和终点之间增加一条“新”边，问题转化为欧拉回路.

根据定理 7-3 知，“七桥问题”无解：不存在欧拉轨迹.

有趣的中国古老数学游戏“一笔画问题”与定理 7-3 密切相关. 所谓一个图能一笔画出是指从图的某节点出发，线可以相交但不能重合，不起笔就可以将图画完.

同样，对于有向图有以下定理.

【定理 7-4】 设 G 是弱连通图，则 G 中存在欧拉轨迹的充要条件是满足下列条件之一.

(1) G 的每节点的入度等于其出度.

(2) G 中存在一个节点出度比入度多 1，存在一个节点入度比出度多 1，而其余所有节点的入度等于其出度.

7.1.3 中国邮递员问题

一位邮递员从邮局选好邮件去投递，然后返回邮局，要求邮递员必须经过其负责的每一条街至少一次，为这位邮递员设计一条投递线路，使总路程最短.

显然，若连通无向图有度数为奇数的节点，由于必须返回邮局，邮递员必须重复走一些街道，问题是怎样才能使得完成投递任务所走的路最短. 这是一个在边赋权的图中允许添加多重边后求最短欧拉回路的问题.

中国邮递员问题(Chinese postman problem)首次由中国图论专家管梅谷于 1962 年提出并研究，提出了“奇偶点图上作业法”，引起世界上不少数学家的关注. 在 1973 年匈牙利数学家 Edmonds 和 Johnson 对中国邮递员问题给出了一种有效算法；另外，在 1995 年王树禾研究了多邮递员中国邮路问题(k-Postman Chinese Postman Problem，k-PCPP)，参见文献[17].

习　题　7.1

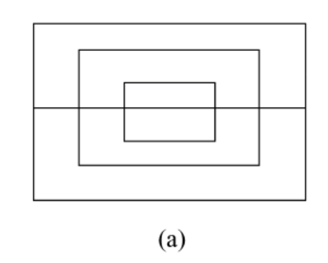
1. 画出分别满足以下条件的欧拉图(n,m).

(1) n 和 m 的奇偶性相同.

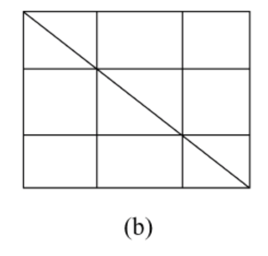
(2) n 和 m 的奇偶性相反.

2. 证明：n 阶完全无向图 K_n 是欧拉图当且仅当 n 为奇数.

3. 判断如图 7-3 所示的图形能否一笔画.



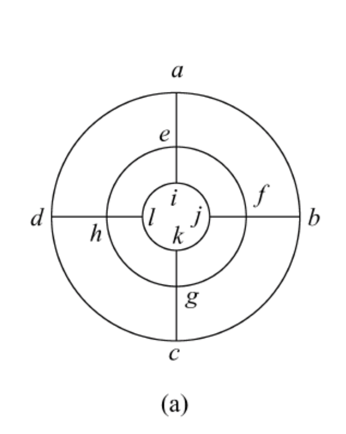
(a)



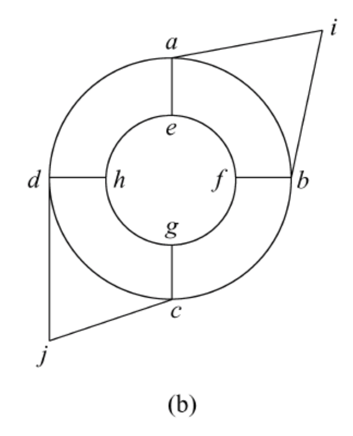
(b)

图　7-3

4. 如图 7-4 所示的两个图各需要多少笔才能画出?



(a)



(b)

图　7-4

5. 如图 7-5 所示的彼得森(Petersen)图至少要加多少条边才能成为欧拉图?试画出添加后的图的图形.若只能添加原图的一些边的多重边,能使得其成为欧拉图?

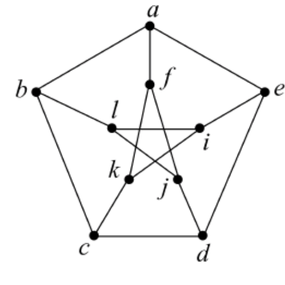


图　7-5

6. 在图 7-3(b)中,给出一种添加多重边的方法,使其成为欧拉图.

7. 在图 7-6 的赋权图中,如何添加多重边才能使其得到的欧拉回路最短?

8. 计算如图 7-7 所示赋权图中的最优投递路线,假定邮局在 C 点.

9. 证明:若无向图 G 恰有两个节点 u 和 v 度数为奇数,则在 G 中 u 可达 v.如果 G 是有向图,上述结论是否成立?

10. 设 $G=(V,E)$是连通无向图,且有 $2k(k\geqslant1)$个度数为奇数的节点,证明:在 G 中存在 k 条轨迹,它们包含了 G 中的所有边.

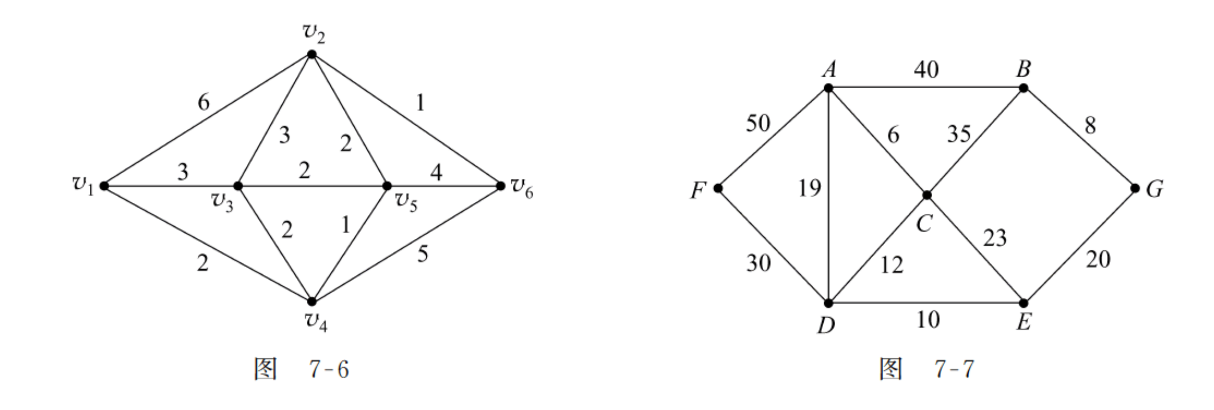


图 7-6 图 7-7

7.2 哈密尔顿图

1859 年爱尔兰数学家哈密尔顿(William Rowan Hamilton,1805—1865)发明了一个周游世界游戏[17]:在一个木制的正 12 面体的 20 个顶点上标示世界上的 20 个大城市,它们分别是北京、莫斯科、东京、柏林、巴黎、纽约、旧金山、伦敦、罗马、里约热内卢、布拉格、新西伯利亚、墨尔本、耶路撒冷、巴格达、上海、布达佩斯、开罗、阿姆斯特丹和华沙.若从一个城市出发,沿正 12 面体的棱旅行,每个城市仅经过一次,最后回到原出发点,就算旅行成功.

这个游戏的发明专利以 25 个金币的高价转让给一个玩具商,据说这个玩具商在几个月内的时间就成了一位腰缠万贯的富豪.

从这个游戏抽象出图论中一种非常重要的哈密尔顿图,且派生出至今为止颇具研究价值的 TSP(Traveling Salesman Problem).

先介绍与哈密尔顿图有关的 3 个概念.

7.2.1 哈密尔顿图的有关概念

【定义 7-2】 设 $G=(V,E)$是任意图,G 中经过所有节点一次且仅一次的路径称为**哈密尔顿路径**(Hamiltonian path),G 中经过所有节点一次且仅一次(除起点重复一次外)的圈称为**哈密尔顿回路**(Hamiltonian cycle)(**哈密尔顿环**或**哈密尔顿圈**),存在哈密尔顿回路的图称为**哈密尔顿图**(Hamiltonian graph)或简称为 H 图.

显然,由哈密尔顿回路可得到哈密尔顿路径,不返回出发点即可,但反过来一般不成立.在图 7-8(a)中的图中存在哈密尔顿路径 $bcaed$,但不存在哈密尔顿回路.

图 7-8(b)中的图存在哈密尔顿回路 $v_1v_5v_4v_3v_2v_1$,它是哈密尔顿图.

注意 欧拉图行遍所有边,而哈密尔顿图行遍所有节点,一般来说有些边不能走到,两者之间没有必然联系.

显然,一个无向哈密尔顿图是连通图,一个有向哈密尔顿图是强连通图.先回到开始时提到的周游世界游戏问题.

【例 7-2】 前面提到的周游世界游戏有解,试加以说明.

解 将正 12 面体投影在平面上得到一个无向图 G,该图存在一条哈密尔顿回路,如图 7-9 所示按顺序从 1 到 2……一直到 20,最后回到 1,所以 G 是哈密尔顿图,故周游世界游戏有解.

判断一个图是否是哈密尔顿图是非常困难的,虽然已经有一些用于判断图是哈密尔顿

图的充要条件，但到目前为止还没有一种方法可以有效地解决哈密尔顿图的判断问题，这是一个计算机科学中的一个 NP 难问题.

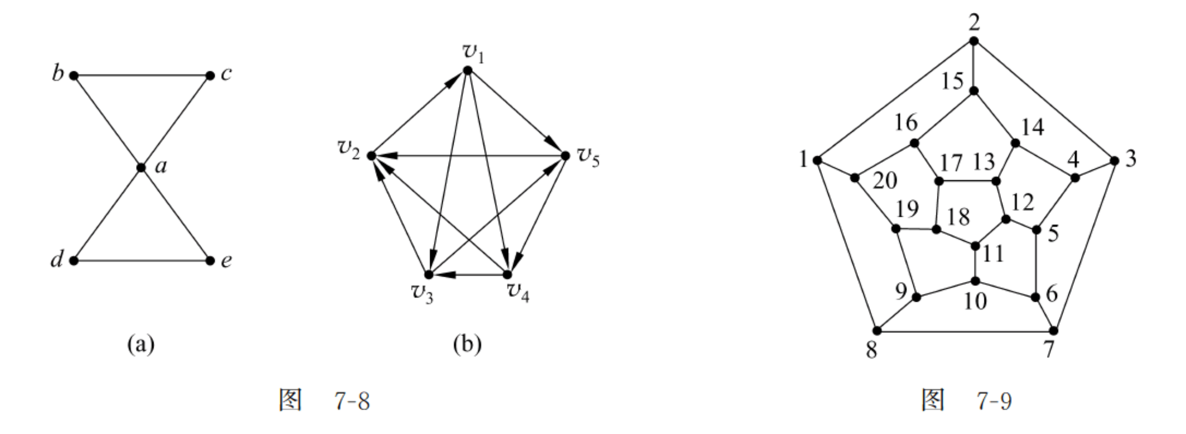


图 7-8　　　　图 7-9

下面分别介绍哈密尔顿图的必要条件和哈密尔顿图的充分条件.

7.2.2 哈密尔顿图的必要条件

【定理 7-5】 设 $G=(V,E)$ 是哈密尔顿无向图，则对于任意 $\varnothing \neq W \subset V$ 均有 $w(G-W) \leqslant |W|$.

证 根据已知条件，G 中存在哈密尔顿回路 C. 显然，$w(G-W) \leqslant w(C-W) \leqslant |W|$.

【例 7-3】 举例说明，定理 7-5 的结论作为条件不是充分的.

解 对于彼得森(Petersen)图，可以验证它不是哈密尔顿图. 如图 7-10 所示说明彼得森图满足定理 7-5 的结论.

在彼得森图中，删除 1 个或 2 个节点都连通；若删除 3 个节点，最多只能得到 2 个连通分支(如图 7-10(a)所示)；若删除 4 个节点，最多只能得到 3 个连通分支(如图 7-10(b)所示)；若删除 5 个节点，剩下的节点数 $\leqslant 5$，当然最多只能得到 5 个连通分支.

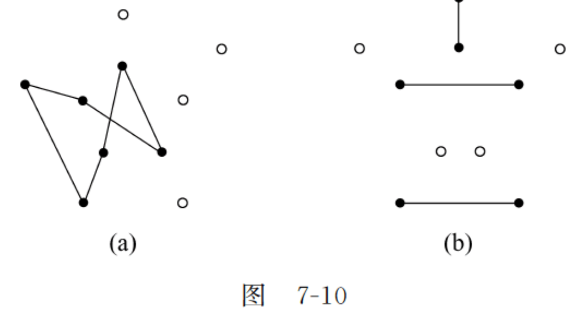


图 7-10

所以，彼得森图满足定理 7-5 的结论，但它不是哈密尔顿图.

7.2.3 哈密尔顿图的充分条件

1960 年 Ore 得到一个哈密尔顿图的充分条件.

【定理 7-6】 (Ore，1960) 设 $G=(V,E)$ 是 $n(n\geqslant 3)$ 阶简单无向图，若对于任意的不相邻节点 u,v 有

$$\deg(u)+\deg(v)\geqslant n$$

则 G 是哈密尔顿图.

证 (1) G 是连通图(参见 6.5 节的例 6-6).

(2) 在 G 中选取一条最长路径 L：$v_1 v_2 \cdots v_{p-1} v_p$，显然 $p \leqslant n$ 且由于 L 最长，分别与 v_1 和 v_p 邻接的节点均在 L 上.

① 如图 7-11 所示,若 v_1 和 v_p 邻接,则由于 L 最长及 G 的连通性知,G 中所有节点都在 L 上,否则会得出一条比 L 长 1 的路径. 这时结论成立.

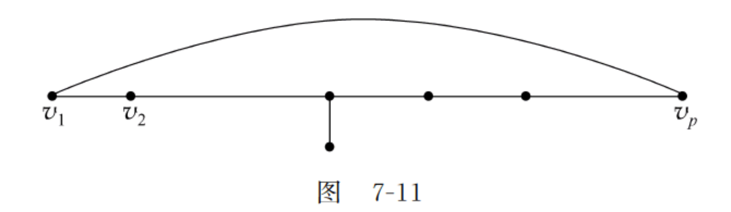


图 7-11

② 若 v_1 和 v_p 不邻接,设与 v_1 邻接的节点分别为 $v_{i_1},v_{i_2},\cdots,v_{i_k}$,若节点 v_{i_1-1},$v_{i_2-1},\cdots,v_{i_k-1}$都不与 v_p 邻接,由于 v_1 和 v_p 不邻接,于是与 v_p 邻接的节点最多有$(n-k)-1$个,因此 $\deg(v_1)+\deg(v_p)\leqslant k+(n-k)-1=n-1$,与已知条件矛盾. 如图 7-12 所示,设 $v_{i_m-1}(1\leqslant m\leqslant k)$与 v_p 邻接,因为 v_1 与 v_{i_m} 邻接,所以路径 L':$v_{i_m}v_1\cdots v_{i_m-1}v_p\cdots v_{i_m+1}$与 L 等长,这时 L'的起点与终点邻接,归结到情形(a).

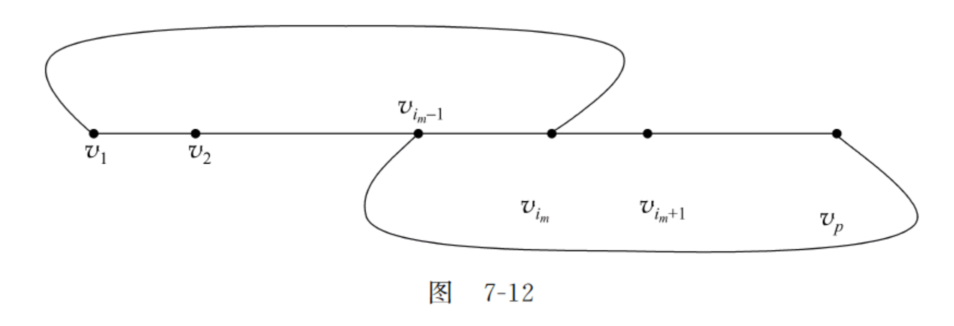


图 7-12

【例 7-4】 举例说明,定理 7-6 的条件不是必要的.

解 对于如图 7-13 所示的图,显然是哈密尔顿图,但任意两个不相邻节点度数之和为 4,而图的阶数为 6.

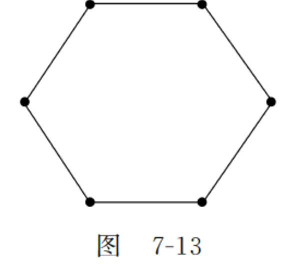


图 7-13

Ore 的上述结果推广了 1952 年 Dirac 的结果.

推论(Dirac, 1952) 设 $G=(V,E)$是 $n(n\geqslant3)$阶简单无向图,若对于任意节点 v 有 $\deg(v)\geqslant n/2$,则 G 是哈密尔顿图.

类似于定理 7-6 有以下定理.

【定理 7-7】 设 $G=(V,E)$是 $n(n\geqslant3)$阶无向图,若对于任意的不相邻节点 u,v 有

$$\deg(u)+\deg(v)\geqslant n-1$$

则 G 中存在哈密尔顿路径.

证(留作练习).

在定理 7-6 的证明过程中,使用了"最长路径法"技巧. 下面再举一个例子说明该方法的使用.

【例 7-5】 设 $G=(V,E)$是 $n(n\geqslant3)$阶连通无向图,证明:G 中存在两个节点,将它们删除后得到的图仍是连通的.

证 在 G 中选取一条最长路径 L:$v_1v_2\cdots v_{p-1}v_p$,由于 L 最长,分别与 v_1 和 v_p 邻接的节点均在 L 上. 考虑 $G-\{v_1,v_p\}$.

假定 $G-\{v_1,v_p\}$不连通,则存在 $G-\{v_1,v_p\}$中两个节点 u_1 和 u_2,它们在 $G-\{v_1,v_p\}$中不可达. 由于 G 是连通的,在 G 中存在一条从 u_1 可达 u_2 的路 L'. 这时 L'必包含 v_1 或 v_p. 而分别与 v_1 和 v_p 邻接的节点均在 L 上,于是在 $G-\{v_1,v_p\}$中必存在 u_1 可达 u_2 的路,这是

一个矛盾. 所以 $G-\{v_1, v_p\}$ 连通.

7.2.4 旅行商问题

有 n 个城镇,其中任意两个城镇间都有道路(若没有则规定该边上的权为 $+\infty$),一个售货员要去这 n 个城镇售货,从某城镇出发,依次访问其余 $n-1$ 个城镇且每个城镇只能访问一次,最后又回到原出发地. 问售货员要如何安排经过 n 个城镇的行走路线才能使他所走的路程最短. 这就是**货郎担问题**或**旅行商问题**(Traveling Salesman Problem,TSP).

求解 TSP 就是要在一个赋权图中,找出一条权最小的哈密尔顿回路. 这是一个比判断一个图是否是哈密尔顿图更困难的问题. 当然,若赋权图是一个三阶及以上的完全无向图,存在哈密尔顿回路是显然的.

求解 TSP,可以先将所有的哈密尔顿回路找出来,再比较其权的大小,求出权最小的哈密尔顿回路即可. 但对于阶数较大的赋权图这样计算的工作量太大. 求货郎担问题的近似解有"近邻法"和"交换法". 目前人们还在研究利用遗传算法、模拟退火算法、神经网络、蚁群算法及粒子群算法等求货郎担问题的近似解的一些智能算法,参见文献[20].

习 题 7.2

1. 如图 7-14 所示,两个图是否为哈密尔顿图?

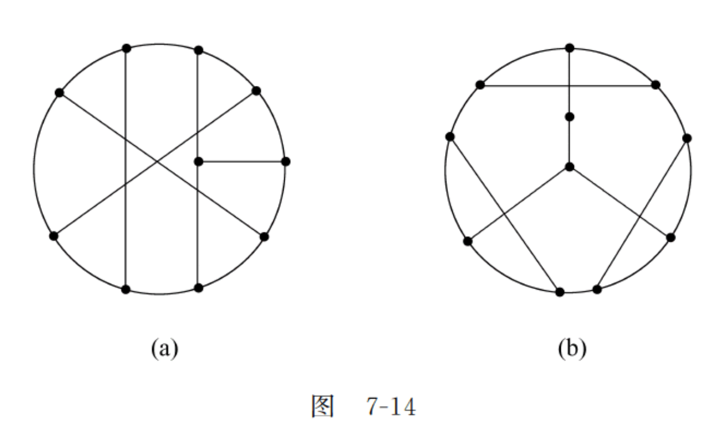


图 7-14

2. 证明:若一个无向图 $G=(V,E)$ 存在一个节点 $v\in V$ 使得 $\deg(v)=1$,则 G 不是哈密尔顿图.

3. 回答下列问题.

(1) 彼得森图不是哈密尔顿图吗? 说明理由.

(2) 可以通过加边使彼得森图成为哈密尔顿图吗? 若可以,试画出添加后的图的图形.

(3) 若只能添加原彼得森图的一些边的多重边,能使得其成为哈密尔顿图吗?

(4) 删除彼得森图的一个节点后所得到的图是否是哈密尔顿图?

4. 分别画出满足下列条件的无向图.

(1) 既是欧拉图又是哈密尔顿图.

(2) 是欧拉图,不是哈密尔顿图.

(3) 不是欧拉图,是哈密尔顿图.

(4) 既不是欧拉图又不是哈密尔顿图.

5. 一只蚂蚁可否从立方体的一个顶点出发,沿着棱爬行,它爬过每一个顶点一次且仅

一次,最后回到原出发点?试利用图作解释.

6. 设 $G=(V,E)$ 是 $n(n\geqslant 3)$ 阶简单无向图.

(1) 若 G 的边数 $m\geqslant C_{n-1}^2+2$,则 G 是哈密尔顿图.

(2) 若 G 的边数 $m=C_{n-1}^2+1$,G 是否一定是哈密尔顿图,说明理由.

7. 有 $n(n\geqslant 4)$ 人,若任意两个人合起来认识其余 $n-2$ 个人,则他们可以站成一个圈,使得每个人的两旁都站着他的朋友.

8. 当 $n\geqslant 3$ 时,K_n 共有多少条不同的哈密尔顿回路?并求出 K_3,K_4,K_5 中各有多少条不同的哈密尔顿回路.

9. 说明如图 7-15 所示的图不是哈密尔顿图.

10. 证明如图 7-16 所示的图不是哈密尔顿图.

11. 求出如图 7-17 所示的赋权图 G 中的权最小的哈密尔顿回路.

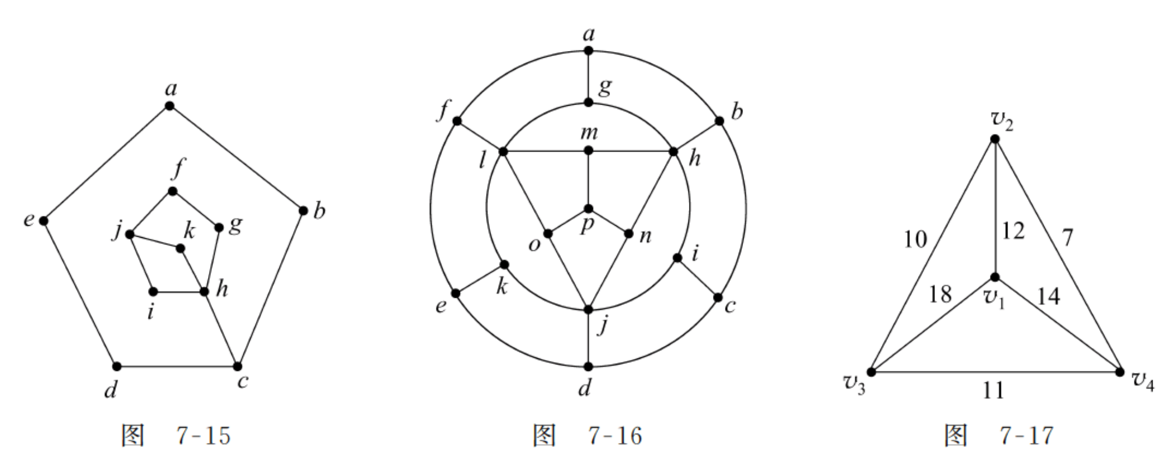


图 7-15　　图 7-16　　图 7-17

7.3 无　向　树

树是图论中的重要内容之一,它是 1847 年 Kirchhoff 在解决电路网络时求解联立方程组时提出来的,可惜他的发现超越了时代,因而长期没有引起重视. A. Cayley 于 1857 年利用树的概念成功研究了有机化学中的同分异构体,从而使无向树的理论获得发展.

目前,树在各个领域都有重要应用,特别是在计算机科学中.

树分为无向树和有向树. 本节仅讨论无向树.

7.3.1 无向树的定义

【定义 7-3】 不含有圈的连通无向图称为**无向树**(tree).

无向树在图论中称为树,也可以称为自由树.

含 $n(n\geqslant 1)$ 个节点的(无向、有向、根)树称为 n 阶(无向、有向、根)树. 不含任意节点的图称为空树.

如图 7-18(a)、图 7-18(b)和图 7-18(c)所示分别是不同结构的一阶无向树、二阶无向树、三阶无向树.

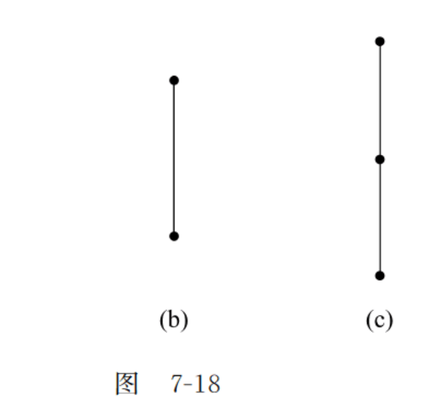


图 7-18

7.3.2 无向树的性质

1. 无向树的基本性质

性质 1 $n(n\geqslant1)$阶无向树恰有 $n-1$ 条边.

证 对 n 使用数学归纳法. 当 $n=1$ 时结论显然成立. 假设 $n\geqslant2$ 且 $n-1$ 阶无向树恰有 $n-2$ 条边.

首先,对于 $n\geqslant2$ 阶无向树 G,每个节点的度数均$\geqslant1$. 由于 G 中不含有圈,由定理 6-3 知必存在一个节点 v,其度数为 1.

考虑 $G-\{v\}$. 由于 G 是不含圈的连通图且 $\deg(v)=1$,所以 $G-\{v\}$是不含圈的连通图,即 $G-\{v\}$是 $n-1$ 阶无向树,它恰有 $n-2$ 条边. 因此,G 恰有 $n-1$ 条边.

【例 7-6】 设 G 是一棵无向树且有 3 个 3 度节点,1 个 2 度节点,其余均为 1 度节点.

(1) 求出该无向树共有多少个节点.

(2) 画出两棵不同构的满足上述要求的无向树.

解 (1) 设 G 有 x 个节点度数为 1,则 G 的节点数为 $x+3+1=x+4$. 由无向树的性质 1 知,G 恰有 $x+3$ 条边.

由握手定理,有 $3\times3+1\times2+x\times1=2(x+3)$,于是 $x=5$. 所以 G 有 9 个节点.

(2) 两棵不同构的满足上述要求的无向树如图 7-19 所示.

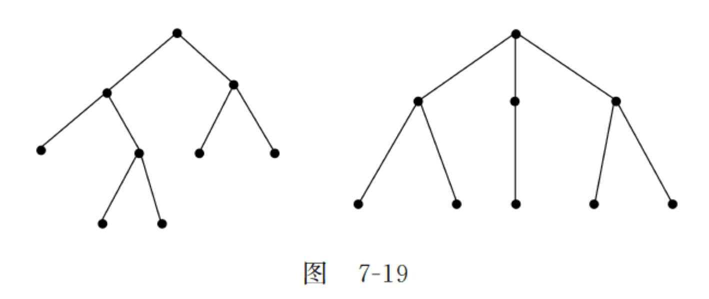


图 7-19

性质 2 $n(n\geqslant2)$阶无向树至少有 2 个度为 1 的节点.

证 由性质 1 的证明过程知,$n(n\geqslant2)$阶无向树 G 至少有 1 个度为 1 的节点. 假定 G 仅有 1 个度为 1 的节点,则其余节点的度数$\geqslant2$,这时 $\sum_v \deg(v)\geqslant 2(n-1)+1$. 而根据性质 1 和握手定理知 $\sum_v \deg(v)=2(n-1)$,这显然是一个矛盾. 故 G 至少有 2 个度为 1 的节点.

【例 7-7】 证明:不同构的四阶无向树 G 仅为如图 7-20所示.

证 根据性质 1,四阶无向树恰有 3 条边,由握手定理知,其所有节点度数之和为 $2\times3=6$. 根据性质 2,四阶无向树至少 2 个度为 1 的节点.

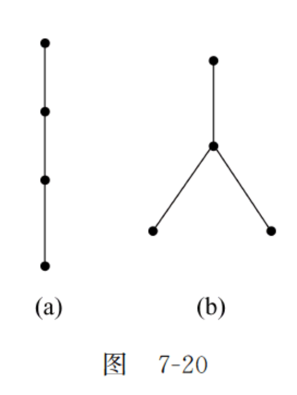


图 7-20

若 G 恰有 2 个度为 1 的节点,则其度数序列为 2,2,1,1,此时为图 7-20(a)中的图.

若 G 恰有 3 个度为 1 的节点,则其度数序列为 3,1,1,1,此时为图 7-20(b)中的图.

2. 无向树的 6 个等价命题

【定理 7-8】 以下关于无向(n,m)图 G 的 6 个命题等价.

(a) G 是一棵无向树.

(b) G 不含有圈且 $m=n-1$.

(c) G 连通且 $m=n-1$.

(d) G 不含有圈但增加一条新边后得到一个且仅一个圈.

(e) G 连通但删除任意一条边后便不连通.

(f) G 的每一对节点有且仅有一条路径.

证 (a)⇒(b) 由性质 1 即得.

(b)⇒(c) 假设 G 不连通，则 G 有 $k(k\geqslant 2)$ 个连通分支，它们都是树，其节点数分别为 $n_1,n_2,\cdots,n_k$，边数分别为 $m_1,m_2,\cdots,m_k$. 由性质 1 知，$m_i=n_i-1,i=1,2,\cdots,k$. 于是

$$m=\sum_{i=1}^{k}m_i=\sum_{i=1}^{k}(n_i-1)=\sum_{i=1}^{k}n_i-k=n-k<n-1$$

与已知矛盾.

(c)⇒(d) 先证明 G 不含有圈，对 n 归纳. 当 $n=1$ 时，边数 $m=0$，显然不含有圈. 假设 $n\geqslant 2$ 且连通 $(n-1,n-2)$ 图没有圈. 对于 G，由于 $m=n-1$，由性质 2 的证明过程知，存在一个度数为 1 的节点 v. 这时，由归纳假设知 $G-\{v\}$ 中没有圈，进而 G 不含有圈.

若在 G 中添加一条边 uv，由于 G 是连通图，在 G 中 u 可达 v. 于是在 $G+uv$ 中存在圈. 若 $G+uv$ 含有 2 个圈，则 G 必含有圈，不可能.

(d)⇒(e) 若 G 不连通，则存在 2 个不可达的节点 u 和 v，当在 G 中添加一条边 uv 后不会出现圈. 若删除一条边后仍连通，则 G 中有圈.

(e)⇒(f) 由连通性知，G 的每一对节点之间有一条路径. 若有 2 条，则 G 中有圈，这时删除圈中的一条边后，G 仍连通，矛盾.

(f)⇒(a) 由于 G 的每一对节点之间有一条路径，于是 G 是连通图. 若 G 中有圈，则圈上的 2 个节点之间存在两条路径.

很容易从上述定理得出无向树的更多性质.

7.3.3 生成树

如图 7-21(a) 所示中的无向图不是无向树，但可以得出其生成子图是无向树，如图 7-21(b)和图 7-21(c)所示.

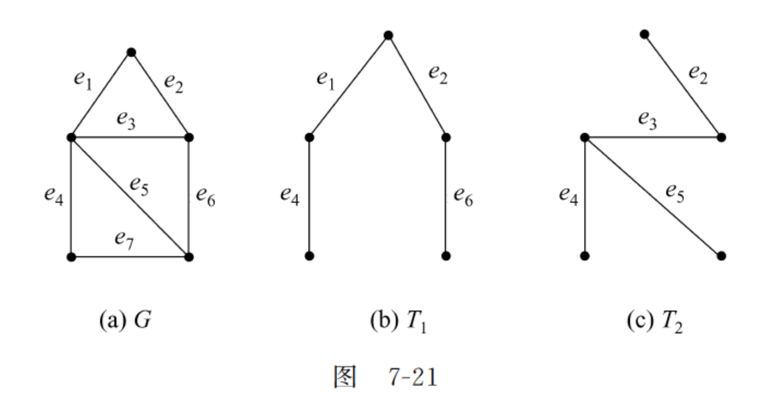


图 7-21

【定义 7-4】 设 $G=(V,E)$ 是无向图，若 G 的生成子图 T 是无向树，则称 T 为 G 的**生成树**(spanning tree).

由图 7-21(b)和图 7-21(c)知，一个无向图的生成树不一定唯一，但不是任意无向图都存在生成树.

【定理 7-9】 设 G 是无向图，则 G 存在生成树的充要条件是 G 是连通图.

证 (⇒)显然.

(⇐)因为 G 连通，若 G 无圈，则 G 本身就是 G 的生成树. 若 G 中存在圈，由定理 7-7 知，删除该圈上的一条边得一个连通生成子图. 继续该过程，一直到没有圈为止. 最后得到的生成子图是一棵无向树，它就是 G 的生成树.

由定理 7-9 有以下推论.

推论 $n(n\geqslant 1)$阶连通图至少有 $n-1$ 条边.

由此可见，$n(n\geqslant 1)$阶无向树是边数最少的连通无向图.

【例 7-8】 设 G 是连通无向图，T 是 G 的任意一棵生成树，C 是 G 的任意圈，则 C 至少含有一条关于生成树 T 中的弦.

证(反证) 若 C 不包含任意关于生成树 T 中的弦，则 C 中的所有边均在生成 T 中，这意味着 T 中含有圈，不可能.

【例 7-9】 设 G 是连通无向图，T 是 G 的任意一棵生成树，F 是 G 的任意边割集，则 F 至少有一条 T 中的树枝.

证(反证) 若边割集 F 不含有生成树 T 中的树枝，则删除 F 中的所有边后，所得到的子图必含有生成树 T，进而是连通的，矛盾.

7.3.4 最小生成树

设 $G=(V,E)$是边赋权的连通无向图，在有些问题讨论中，不但要得出 G 的一棵生成树，而且要求生成树各边的权之和最小.

【定义 7-5】 设 G 是一个边赋权的连通无向图，G 的生成树各边的权之和称为该生成树的权，G 中权最小的生成树称为**最小生成树**(minimal spanning tree).

下面分别介绍求边赋权的连通无向(n,m)图的最小生成树的算法.

算法 1 克鲁斯卡尔(Kruskal，1956)的避圈法

先将图 G 的 m 条边，按权从小到大的顺序排列：$e_1,e_2,\cdots,e_m$. 按从左至右顺序

(1) 选取第一条边 e_{i_1}，只要 e_{i_1} 不构成圈，令 $j\leftarrow 1$.

(2) 若 $j=n-1$，则算法结束，否则转向(3).

(3) 假定已经选取了 $e_{i_1},e_{i_2},\cdots,e_{i_k}$，再选取 $e_{i_{k+1}}$，只要$\{e_{i_1},e_{i_2},\cdots,e_{i_k},e_{i_{k+1}}\}$不构成圈. 令 $j\leftarrow j+1$，转向(2).

Kruskal 的避圈法的基本思想是：以边的权从小到大的顺序，逐步选边，但必须去掉产生圈的边，即避开圈的产生，直至得到 $n-1$ 条边为止. 算法的正确性是显然的.

【例 7-10】 使用 Kruskal 的避圈法，求出如图 7-22(a)所示边赋权图 G 的最小生成树.

解 按 Kruskal 的避圈法可得出其最小生成树 T 为如图 7-22(b)所示.

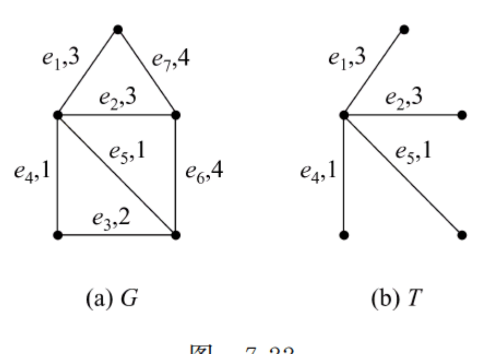


图 7-22

算法 2　普里姆(Prim, 1957)算法

基本思想：从任意节点出发，选取与其关联且权最小的边以及该边的另一个关联节点，两点及边构成一个图 H. 在 $G-H$ 中选取与 H 中所有节点关联的最小权的边及另一个与该边关联的节点，将它们全并入 H. 继续该过程，直到 H 包含了 G 的所有节点.

算法 3　管梅谷(1975)的破圈法

基本思想：在 G 中任意选取一个圈，去掉该圈上的最大权的一条边，直到不含圈为止.

习　题　7.3

1. 分别画出所有不同构的五阶无向树和六阶无向树.

2. 设 G 是一棵无向树且有 2 个 4 度节点，3 个 3 度节点，其余均为叶节点.

(1) 求出该无向树共有多少个节点.

(2) 画出两棵不同构的满足上述要求的无向树.

3. 设 G 是一棵无向树且有 n_i 个 i 度节点，$i=2,3,\cdots,k$，其余均为叶节点，求叶节点的个数.

4. 证明：连通无向图 G 是无向树的充要条件是 G 的每一条边都是桥.

5. 设 G 是无向树且 $\Delta(G)\geqslant k$，则 G 至少有 k 片树叶.

6. 证明：恰有两片树叶的无向树是一条路径.

7. 如图 7-23(a)和图 7-23(b)所示的两个图，分别画出所有不同构的生成树.

8. 求出 K_6 中所有不同构的生成树.

9. 求出如图 7-24 所示边赋权图 G 的最小生成树的权.

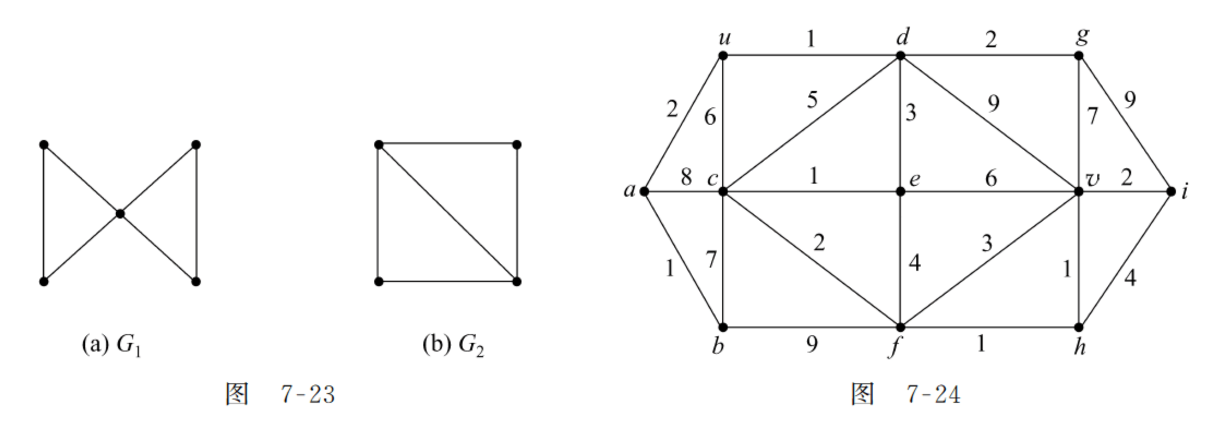


图　7-23　　　　图　7-24

10. (1) 证明：n 阶无向树的所有节点度数之和为 $2(n-1)$.

(2) 设 $d_1,d_2,\cdots,d_n$ 是 n 个正整数($n\geqslant 2$)，若 $\sum_{i=1}^{n} d_i=2(n-1)$，则存在一棵无向树，其节点度数分别为 $d_1,d_2,\cdots,d_n$.

7.4　有　向　树

在 7.3 节讨论的是无向树，本节讨论有向树的有关内容，它们在计算机算法设计及程序设计研究中都起着重要作用.

7.4.1 有向树的定义

【定义 7-6】 一个有向图 $G=(V,E)$，在不考虑边的方向时是一棵无向树，则该有向图称为**有向树**(directed tree).

如图 7-25 所示是两个有向树的例子.

在一棵有向树中，节点 v 的前驱元素称为 v 的**父节点**(parent)，v 的后继元素称为 v 的**子节点**(child).实际上，在一个**无环有向图**(directed acycline graph，DAG)中均可以定义父节点和子节点，若有向边 $(u,v)\in E$，则称 u 是 v 的父节点，v 是 u 的子节点.

如图 7-26 所示是两个无环有向图的例子. 一般说来 DAG 不是有向树，但它常用在讨论拓扑排序及关键路径中. 量子线路就是无环有向图，因为它不需要利用反馈信息.

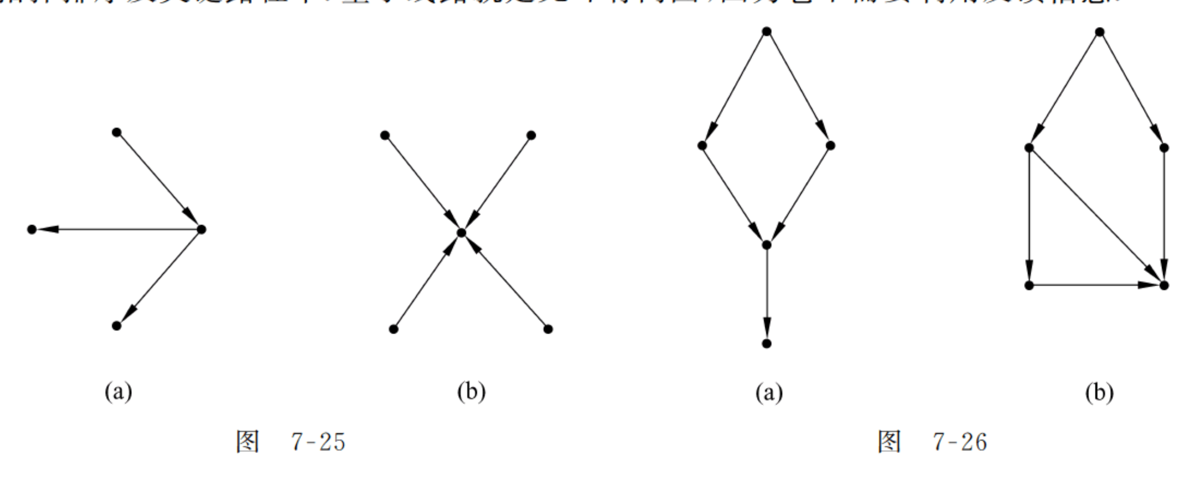


图 7-25 (a) (b)　　图 7-26 (a) (b)

7.4.2 根树

在有向树中，更常用的是根树，它能清楚地表示层次结构. 在编译程序中，用于表示源程序的语法结构，在数据库系统中用于表示信息的组织形式.

【定义 7-7】 一棵有向树，若恰有一个节点入度为 0，而其余节点入度均为 1，则该有向树称为**根树**(rooted tree).

注意 根树在计算机科学中常称为树，其他概念在含义上也有些细微不同.

如图 7-27 所示是两棵根树的例子.

在根树中，入度为 0 的节点称为**树根**(root)，出度为 0 的节点称为**树叶**(leaf)，出度不为 0 的节点称为**分支节点**，将不是根的分支节点称为**内点**.

一般将根树的根画在上方或下方，这时边的方向都朝下(如图 7-27(a)所示)或都朝上(如图 7-27(b)所示). 正因为这样，在实际应用中，根树的方向是可以省略的.

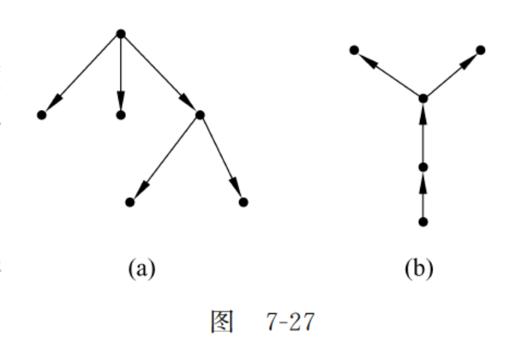


图 7-27 (a) (b)

为了方便，可以借助于家族树称呼根树中的节点. 若有向边 $(u,v)\in E$，则称 u 是 v 的**父节点**(parent)，v 是 u 的**子节点**(child). 同一个父节点的子节点称为**兄弟节点**(sibling). 节点的**祖先**(ancestor)是从根节点到该节点的路径上所经过的所有分支节点. 从一个节点可以到达别的任意节点都称为该节点的**后代**(offspring 或 descendants).

可以证明,从根节点到任意节点有且仅有一条路径.从根节点到某个节点的路径的长度称为该节点的**层**或**级**(level).于是,根节点是第0层节点,其子节点称为第1层节点,以此类推.其父节点在同一层的节点互为**堂兄弟**.根树中节点的最大层次,称为根树的**高度**(height)或**深度**(depth).

在根树中,所有树叶的层数之和称为该根树的**外部路径长度**,记为 E;所有内点的层数之和称为该根树的**内部路径长度**,记为 I.

【定义 7-8】 设 $G=(V,E)$是一棵根树,$v\in V$,由节点 v 及其所有后代导出的子图称为 G 的**子根树**(rooted subtree),可以简称为**子树**(subtree).

可以结合如图7-28[21]中所示的根树理解上面提到的概念.需要注意的是,关于根树中节点的**层**(level)的含义在有些数据结构中有所不同,它们将根节点称为第1层节点,其子节点称为第2层节点,以此类推.

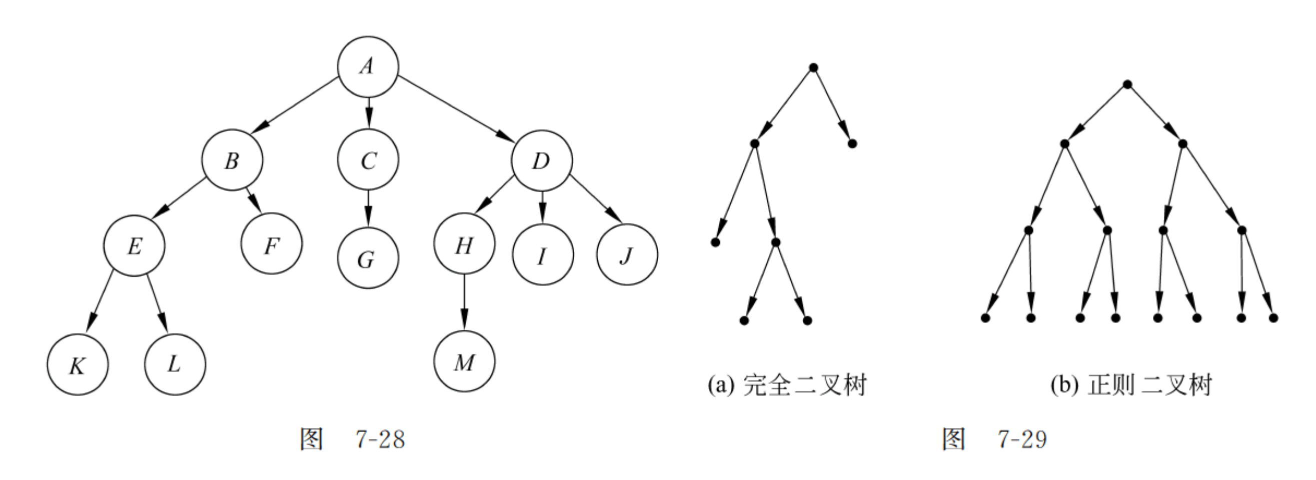


图 7-28　　　　图 7-29

7.4.3 *m* 叉树

在根树中,一个节点的出度可以称为**元**,或更形象地称为**叉**.在数据结构中有称为"度"的,但容易与图论中节点的度数概念混淆.当然,用根树的最大出度称呼其名有时会更直观、方便.

1. *m* 叉树的定义

【定义 7-9】 设 $G=(V,E)$是一棵根树,若$\max\limits_{v\in V}\mathrm{od}(v)=m$,则称 G 是 ***m* 叉树**(m-ary tree).

如图7-28所示是一棵3叉树.如图7-27(b)所示是一棵二叉树,但要与数据结构中的二叉树相区别,见下面关于二叉树的进一步说明.

在 m 叉树 G 中,若对于任意节点 v 均有$\mathrm{od}(v)=m$ 或0,则称 G 为**完全 *m* 叉树**,所有树叶节点所在的层都相同的完全 m 叉树称为**正则 *m* 叉树**,或称为**满 *m* 叉树**.

如图7-29(a)所示是一棵完全二叉树,如图7-29(b)所示是一棵正则二叉树.

2. *m* 叉树的性质

下面是有关 m 叉树的几条性质,这些性质在数据结构中也有讨论.

性质1 　m 叉树的第 i 层的节点至多为 m^i($i\geqslant 0$).

证 　对层数 i 归纳.当 $i=0$ 时,第0层节点仅为树根,有 $m^0=1$,结论成立.设第$i-1$层节点至多 m^{i-1},因为每个节点的出度均$\leqslant m$,从而第 i 层的节点至多 $m\cdot m^{i-1}=m^i$.

显然,正则 m 叉树的第 i 层的节点恰为 $m^i(i\geqslant 0)$.

性质 2 高度为 h 的 m 叉树至多有 $(m^{h+1}-1)/(m-1)(m\geqslant 2)$ 个节点.

证 由性质 1 知结论成立.

性质 3 一棵有 l 片树叶的 m 叉树的高度至少为 $\log_m l$.

证 当所有 l 片树叶处于同一层且分支点的儿子数等于或尽可能接近 m 时,该 m 叉树的高度最小. 对于高度为 h 的 m 叉树,由性质 1 知 $l\leqslant m^h$,所以 $h\geqslant \log_m l$.

性质 4 若一棵完全 m 叉树有 l 片树叶、t 个分支节点,则 $(m-1)t=l-1$.

证 有 t 个分支节点的完全 m 叉树有 mt 条边、$t+l$ 个节点,于是 $mt=t+l-1$,因此 $(m-1)t=l-1$.

下面是二叉树的几条性质.

性质 5 若二叉树有 l 片树叶,则出度为 2 的节点有 $l-1$ 个.

证 设出度为 1 的节点有 x 个,出度为 2 的节点有 y 个,则该二叉树有 $x+y+l$ 个节点、$x+y+l-1$ 条边. 显然,所有出度之和等于边数,即

$$x+2y=x+y+l-1$$

于是,有 $y=l-1$.

性质 6 有 l 片树叶的完全二叉树有 $2l-1$ 个节点.

证 由性质 4 知结论成立.

性质 7 若完全二叉树有 t 个分支节点,则 $E=I+2t$,其中 E 为外部路径长度,I 为内部路径长度.

证 设该完全二叉树有 l 片树叶,则由性质 5 知 $t=l-1$. 对 t 归纳. 当 $t=0,1$ 时,结论显然成立.

假设对于分支节点个数小于 t 的完全二叉树结论成立. 对于分支节点个数为 t 的完全二叉树,去掉根节点得到两棵完全二叉树,其外部路径长度、内部路径长度和分支节点个数分别为 E_1,I_1,t_1 和 E_2,I_2,t_2,根据归纳假设有 $E_1=I_1+2t_1$ 且 $E_2=I_2+2t_2$. 由于$E=E_1+E_2+l$,$I=I_1+I_2+(t-1)$且 $t_1+t_2=t-1$,因此

$$\begin{aligned}E&=(I_1+2t_1)+(I_2+2t_2)+l=I_1+I_2+2(t_1+t_2)+l\\&=I_1+I_2+2(t-1)+l=(I_1+I_2+(t-1))+(t-1)+l\\&=I+(t-1)+l=I+t+(l-1)=I+2t\end{aligned}$$

3. 叶赋权 m 叉树

下面讨论叶赋权 m 叉树.

【定义 7-10】 设 $G=(V,E)$是一棵 m 叉树,若 G 的每一片树叶上都赋予一个非负实数,则称 G 为**叶赋权 m 叉树**.

可以将树叶理解为苹果,树叶上所赋的权理解为苹果的质量.

【定义 7-11】 设 $G=(V,E)$是一棵叶赋权 m 叉树,其 l 片树叶上的权分别为 w_1,w_2,…,w_l,记根节点到权为 w_i 的树叶节点的路径长度(即距离)为 $L(w_i)(i=1,2,\cdots,l)$,称 $\sum\limits_{i=1}^{l} w_i\cdot L(w_i)$ 为 m 叉树 G 的**权**,记为 $W(G)$.

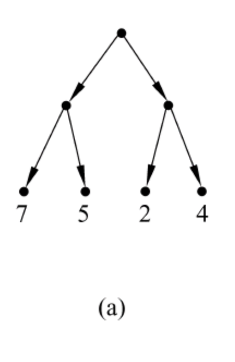
可以将 m 叉树 G 的权 $W(G)$理解为 m 叉树 G 的承受"力",也可借助于后面的 Huffman 编码帮助理解.

如图 7-30(a)～图 7-30(c)所示的 3 棵二叉树的权分别为

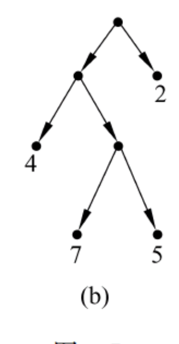
$$7\times 2+5\times 2+2\times 2+4\times 2=36$$

$$7\times 3+5\times 3+2\times 1+4\times 2=46$$

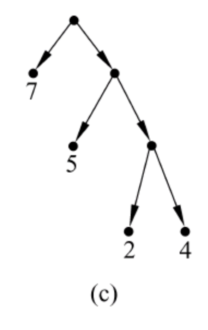
$$7\times 1+5\times 2+2\times 3+4\times 3=35$$



(a)



(b)



(c)

图 7-30

下面仅讨论最优二叉树问题，它在解决某些判定问题时可以得到最佳判定算法. 所得结论可以推广到一般的最优 m 叉树.

【定义 7-12】 设 $G=(V,E)$ 是一棵叶赋权二叉树，其 l 片树叶上的权分别为 w_1，w_2，…，w_l，在所有树叶数相同以及相应树叶上的权也相同的二叉树中，权最小的那棵称为**最优二叉树**或**赫夫曼树**.

赫夫曼(Huffman)在 1952 年首先给出一个求最优二叉树的有效算法，其基本思想是，将给定的 l 片树叶上的权按从小到大的顺序排列，不妨设为 $w_1\leqslant w_2\leqslant\cdots\leqslant w_l$；分别赋权为 $w_1,w_2,\cdots,w_l$ 的 l 片树叶的最优二叉树可以从有 $l-1$ 片树叶，且权分别为 $w_1+w_2,w_3,\cdots,w_l$ 的最优二叉树得到；再将 $w_1+w_2,w_3,\cdots,w_l$ 按从小到大顺序排列，继续以上步骤即可得所求的最优二叉树.

【例 7-11】 计算有 5 片树叶，分别赋权 1，2，3，4，5 的赫夫曼树.

解 对于 1，2，3，4，5，先组合两个最小的权 1+2=3，得 3，3，4，5；在所得到的序列中再组合 3+3=6，重新排列后为 4，5，6；再组合 4+5=9，得 6，9；最后组合 6+9=15.

$$\begin{array}{ccccc}\underline{1} & \underline{2} & 3 & 4 & 5\\ & \underline{3} & \underline{3} & 4 & 5\\ & & 6 & \underline{4} & \underline{5}\\ & & \underline{6} & & \underline{9}\\ & & & & 15\end{array}$$

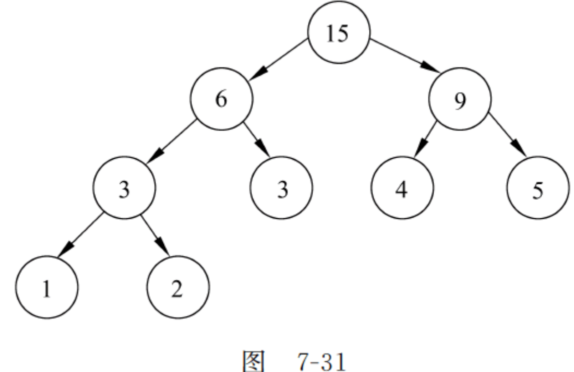


图 7-31

所求的赫夫曼树如图 7-31 所示.

赫夫曼算法的正确性是比较显然的.

7.4.4 有序树

在根树中，对同一个节点的所有儿子节点是没有先后顺序的，这与家族树不太一致. 同时，在有些应用问题中，需要对同一个节点的所有儿子节点规定一个先后顺序，通常是从左至右顺序，这就是有序树.

【定义 7-13】 设 $G=(V,E)$ 是一棵根树，若对同一个节点的所有儿子节点规定一个先后顺序，则称 G 为**有序树**(ordered tree).

在有序树中，一个节点的最左边的儿子常称为该节点的**长子**. 在同一个父节点的所有子节点中，一个节点的右边第一个节点称为该节点的**大弟**. 如果一片森林中，每一棵树都是有序树，且全体有序树的根也规定了先后顺序，则称该森林为**有序森林**(ordered forest)，其中一棵有序树的右边第一棵有序树的根是前一棵有序树的根的**大弟**.

【例 7-12】 用有序树表示表达式 $(a-b)/|c|$.

解 $(a-b)/|c|$ 的有序树表示如图 7-32(a)所示.

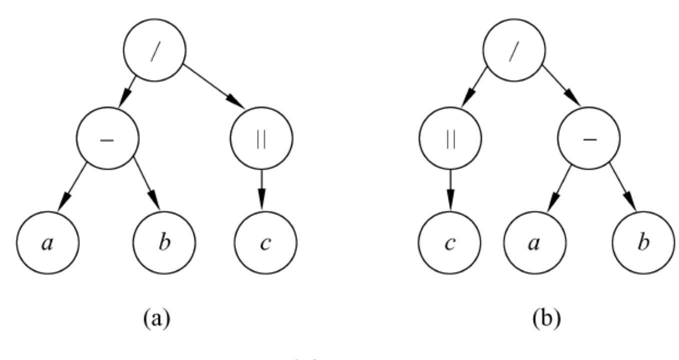


图 7-32

注意 在图 7-32(a)与图 7-32(b)中，作为根树它们是同构的，但作为有序树它们是不同的，因为图 7-32(b)表示的是 $|c|/(a-b)$.

7.4.5 定位二叉树

对于二叉有序树，每个分支节点至多两个儿子. 若对这两个儿子，包括只有一个儿子的情形，还根据实际情况确定了其左右位置，分别称为**左儿子**和**右儿子**，这就是定位二叉树.

1. 定义

【定义 7-14】 设 $G=(V,E)$ 是一棵有序二叉树，若对同一个节点的所有儿子节点规定一个左右位置，则称 G 为**定位二叉树**(positional binary tree).

如图 7-33 所示是两棵二叉树，作为有序树它们是相同的. 作为定位二叉树是不同的，因为在图 7-33(a)中，v 是 u 的左儿子，而在图 7-33(b)中，v 是 u 的右儿子.

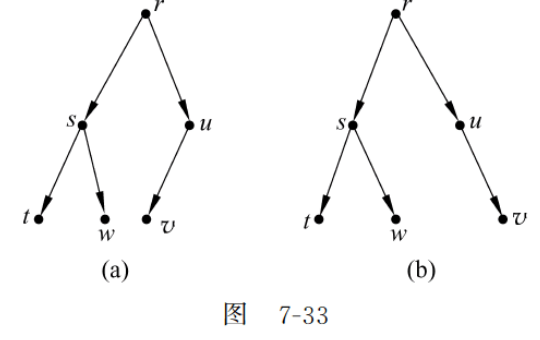


图 7-33

这里的定位二叉树是数据结构中的二叉树(binary tree)，它要区分左儿子和右儿子，进而有左子树和右子树之分. 在图 7-33(a)中，r 的左子树是由 s,t,w 导出的子图，r 的右子树是由 u,v 导出的子图；u 的左子树是 v，u 不存在右子树.

2. 赫夫曼编码

在定位二叉树中，与赫夫曼树密切相关的是赫夫曼编码. 现给出前缀及前缀码的定义.

【定义 7-15】 设 $\beta=\alpha_1\alpha_2\cdots\alpha_n$ 是长度为 n 的符号串，则称子串 $\alpha_1,\alpha_1\alpha_2,\cdots,\alpha_1\alpha_2\cdots\alpha_{n-1}$ 分别为 β 的长度为 $1,2,\cdots,n-1$ 的**前缀**(prefix). 设 $A=\{\beta_1,\beta_2,\cdots,\beta_m\}$ 是符号串组成的集合，

若对于任意 $i \neq j$ 均有 β_i 与 β_j 互不为前缀,则称 A 为**前缀码**(prefix code).若 $\beta_i(i=1,2,\cdots,m)$ 中只出现 0 或 1 两个符号,则称 A 为**二元前缀码**(binary prefix code).

用二进制对计算机及通信中使用的符号进行编码时,一要保证编码没有歧义,不会将字母传错,二要保证码长要尽可能地短.使用定位二叉树,可以将节点的左儿子所在边标记为 0,而将右儿子所在边标记为 1,则可以产生唯一的树叶的二进制编码作为通信的符号编码就不会产生歧义,并且是二元前缀码.

【例 7-13】 分别求出如图 7-34 所示的定位二叉树得到的二元前缀码.

解 将定位二叉树每个分支节点与其左儿子所在的边标为 0,与其右儿子所在的边标为 1,则图 7-34(a)和图 7-34(b)所得到的二元前缀码分别为{00,01,10}和{00,01,11}.

为了保证码长要尽可能地短,使用赫夫曼编码即可.**赫夫曼编码**是使得电文总长最短的二进制前缀编码,其叶上的权为传输各符号的频率,所得到的赫夫曼树的权为传输一个符号需要使用的二进制数字的个数.

【例 7-14】 将 7 个符号按其出现的频率 0.2, 0.19, 0.18, 0.17, 0.15, 0.1, 0.01 构造其赫夫曼编码.

解 先根据叶上的权为传输各符号的频率,得到一棵赫夫曼树,如图 7-35 所示,其叶节点的编码即为赫夫曼编码:{00,01,1000,1001,101,110,111}.

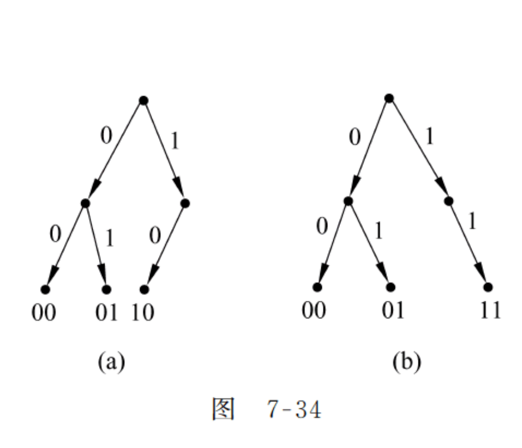


图 7-34

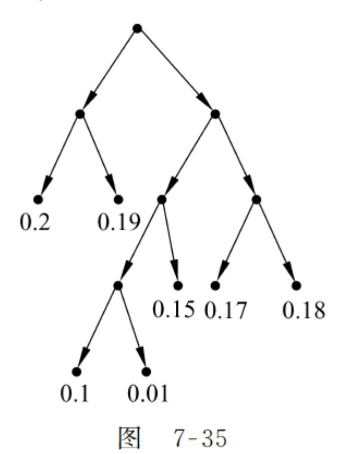


图 7-35

这样得到的赫夫曼编码是最佳二元前缀码,其码长为 4,而该定位二叉树的权为

$$2\times0.2+2\times0.19+4\times0.1+4\times0.01+3\times0.15+3\times0.18+3\times0.17=2.72,$$

它表示传 1(或 100)个按上述频率出现的符号需要 2.72(或 272)个二进制数字.

3. 遍历方式

遍历定位二叉树(traversing binary tree)有 3 种方式(如图 7-36 所示):

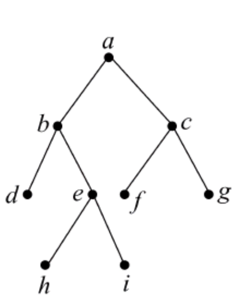


图 7-36

(1) 前序遍历:根节点→左子树→右子树:*abdehicfg*.

(2) 中序遍历:左子树→根节点→右子树:*dbheiafcg*.

(3) 后序遍历:左子树→右子树→根节点:*dhiebfgca*.

4. 有序森林与定位二叉树之间的转换

由于定位二叉树结构简单,因此经常将有序森林,特别是有序树,转换成定位二叉树,并以有序森林与定位二叉树之间的转换作为结束.

在有序森林 F 与定位二叉树 B 之间根据自然转换规则建立一一对应：

(1) 在 F 中 u 是 v 的长子，则在 B 中 u 是 v 的左儿子.

(2) 在 F 中 u 是 v 的大弟，则在 B 中 u 是 v 的右儿子.

【例 7-15】 将图 7-37(a)中的有序森林 F 转换成定位二叉树 B.

解 按自然转换规则得到的定位二叉树 B 如图 7-37(b)所示.

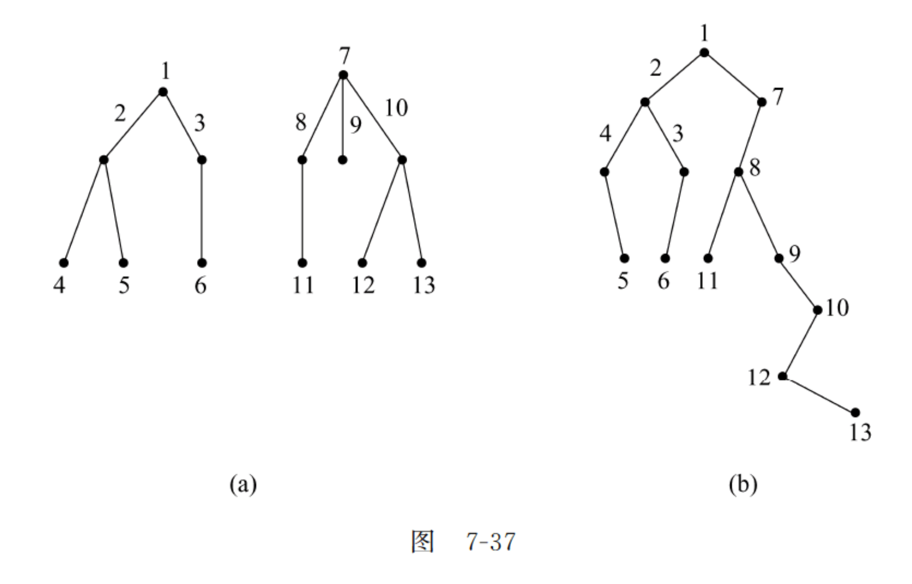


图 7-37

习 题 7.4

1. 证明：在根树中，从树根到任意节点有且仅有唯一的一条路径(提示：对节点所在的层归纳).

2. 画出所有不同构的 4 阶根树及 5 阶根树.

3. 指出图 7-28 中的根树 T 的下列节点.

(1) 根节点.

(2) 树叶节点.

(3) 分支节点.

(4) 内点.

(5) 每个节点的层.

(6) 每个节点的父节点.

(7) 每个节点的子节点.

(8) 树高.

(9) 最大出度.

(10) 所有子(根)树.

4. 如图 7-26 所示，存在是根树的生成子图吗？若存在，求出所有不同构的是根树的生成子图.

5. 证明：高度为 h 的 m 叉树至多有$(m^{h+1}-1)/(m-1)(m\geqslant 2)$个节点.

6. 证明以下结论：

(1) 完全二叉树的节点个数必是奇数；

(2) n 阶完全二叉树的树叶的数目为$(n+1)/2$；

(3) n 阶完全二叉树的树高为$\lfloor \log_2 n \rfloor$,其中$\lfloor x \rfloor$表示小于等于 x 的最大整数.

7. 设 G 是有 t 个分支节点、l 片树叶、高为 h 的正则 m 叉树,则

(1) G 有 $mt+1$ 个节点.

(2) $l=t(m-1)+1$.

(3) $l \geqslant h(m-1)+1$.

8. 计算有 13 片树叶,分别赋权 2,3,5,7,11,13,17,19,23,29,31,37,41 的赫夫曼树,并构造最优三叉树.

9. 用有序树分别表示表达式 $v_1 v_2-(v_4+v_5/v_6)v_3$ 和 $a+b(c-d)-e/f$.

10. 在下面给出的 3 个符号串集合中,哪些是前缀码？哪些不是前缀码？若是前缀码,则构造定位二叉树,其树叶代表其二进制编码.若不是前缀码,则说明理由.

(1) $A_1=\{0,10,110,1111\}$.

(2) $A_2=\{1,01,001,0000\}$.

(3) $A_3=\{1,11,101,001,0011\}$.

11. 在通信中,八进制数字 0,1,2,3,4,5,6,7 出现的频率分别为 0：30%,1：20%,2：15%,3：10%,4：10%,5：6%,6：5%,7：4%.编写一个传输它们的最佳前缀码,使通信中出现的二进制数字尽可能地少.具体要求如下：

(1) 画出相应的赫夫曼树；

(2) 写出每个数字对应的前缀码；

(3) 传输上述比例出现的数字 10 000 个时,至少要用多少个二进制数字？

12. 将如图 7-38 所示的有序森林 F 转换成定位二叉树 B.

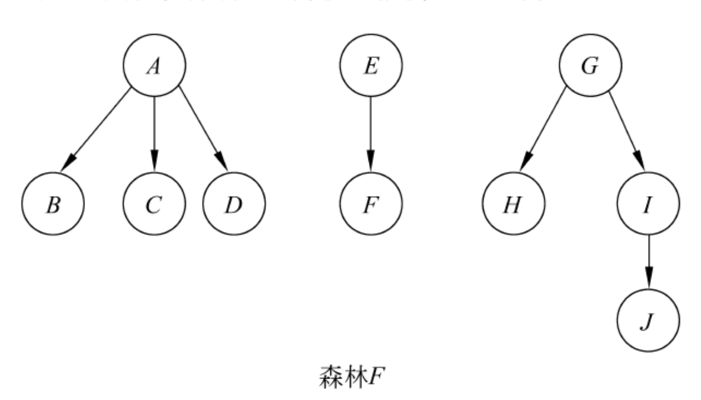


图 7-38

7.5 平 面 图

本节仅讨论无向图.

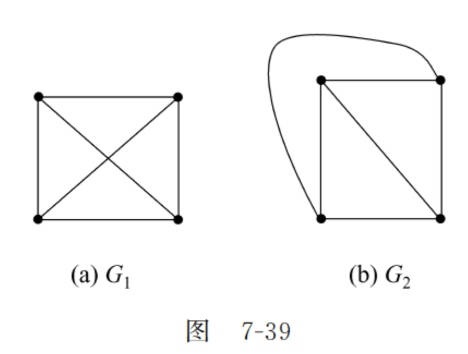
对于一个无向图,怎样将其图形画出来本身是无关紧要的,只要与原来的图同构皆可.但有些实际问题要求把图画在一个平面上,同时使得图的边在非节点处不相交.例如单层印刷电路板、集成电路的布线等问题就需要满足上面的要求.

虽然在现实生活中出现了交通立交桥、多层电路板,但平面图问题仍然是基本问题.例如在上章 7.1 节提到的"3 户 3 井问题"就是判定一个图是否是平面图的问题.

平面图与地图着色问题密切相关.

7.5.1 平面图的有关概念

【定义 7-16】 设 G 是无向图,若可将 G 画在一个平面上,同时使得任意两条边在非节点处不相交,则称 G 是**可平面图**(planar graph)或简称 G 为**平面图**(plane graph).



(a) G_1 (b) G_2

图 7-39

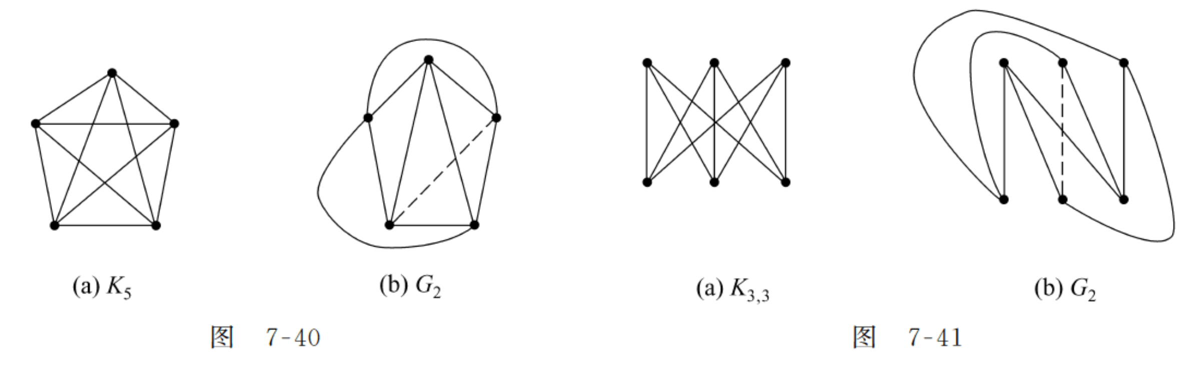
设 G 是平面图,则可在一个平面上将图 G 画出来且使得其任意两条边仅仅在节点处才相交,这样画出的图称为平面图 G 的**平面嵌入**(planar embedding)或平面表示.由于一个平面图与其平面表示是同构的,因此平面图通常是指其平面表示.

如图 7-39 中所示的图 G_1 和 G_2 都是平面图.显然,G_2 也是平面图 G_1 的平面嵌入或平面表示.

两个重要的非平面图的例子.

(1) K_5,如图 7-40 所示.

(2) $K_{3,3}$,如图 7-41 所示.



(a) K_5 (b) G_2

图 7-40

(a) $K_{3,3}$ (b) G_2

图 7-41

【定义 7-17】 设 G 是简单平面图,若在 G 的任意两个不相邻的节点 u 和 v 之间增加一条边所得到的图 $G+uv$ 是非平面图,则称 G 为**极大平面图**(maximal planar graph).

显然,若 e 是 K_5 的一条边,则 $K_5-\{e\}$ 是极大平面图.但是,若 e 是 $K_{3,3}$ 的一条边,则 $K_{3,3}-\{e\}$ 不是极大平面图.

【定义 7-18】 设 G 是非平面图,若在 G 中任意删除一条边所得到的图是平面图,则称 G 为**极小非平面图**(minimal nonplanar graph).

容易看出,K_5 和 $K_{3,3}$ 都是极小非平面图.

【定义 7-19】 设 G 是平面图,由 G 的若干条边所围成的连通区域称为图 G 的**面**(face),围成面的回路称为面的**边界**(boundary).

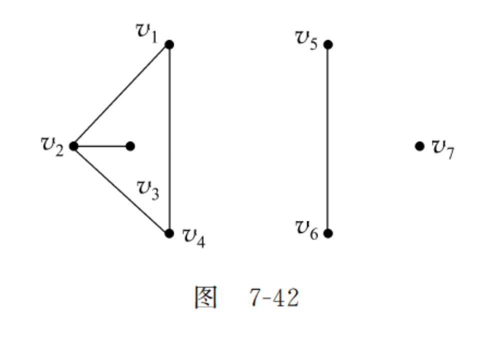


图 7-42

一个区域是连通的,是指其内部可随意走动而不穿过任何边.在图 7-39(b)中有 4 个面.如图 7-42 所示中的平面图有 2 个面,分别是由 $v_1v_2v_3v_2v_4v_1$ 往内围成一个面,$v_1v_2v_4v_1+v_5v_6v_5$ 往外围成一个面.

特别注意,任何平面图都有一个由若干条边往外围成的一个面,它是唯一的一个无限面.

求一个平面图的面可以这样做,在一张较大的纸上将平面图画上,然后用剪刀将图的所

有边剪破，这张纸被分成的每一部分就是一个面.

平面图的两个面相邻是指这两个面有公共的边界.

7.5.2 欧拉公式

欧拉在 1750 年研究多面体时发现，多面体的面数等于多面体的棱数减去顶点数加 2，后来发现连通平面图的面数与其节点数、边数之间也有同样的关系.

【定理 7-10】 （欧拉公式）任意(n,m)连通平面图 G 的面数 $r=m-n+2$.

证 对 G 的面数 r 归纳. 当 $r=1$ 时，G 只有一个无限面，进而 G 不含任何圈. 因为 G 连通，所以 G 是一棵无向树，进而由无向树的性质 1 知 $m=n-1$，于是有 $r=m-n+2$.

假设 $r-1$ 是成立. 由于 $r\geqslant 2$，G 中存在简单回路 C，令 e 是 C 上的一条边，考虑 $G-\{e\}$. 显然，$G-\{e\}$是一个连通的平面图. 因为 $G-\{e\}$的面数为 $r-1$，根据归纳假设有 $r-1=(m-1)-n+2$，所以有 $r=m-n+2$.

注意 在欧拉公式中，“连通”的条件是必不可少的. 在图 7-42 中，$r=2$，而 $m-n+2=5-7+2=0$.

下面的推论非常有用.

推论 1 任意(n,m)简单连通平面图，若 $n\geqslant 3$，则 $m\leqslant 3n-6$.

证 设 G 是(n,m)简单平面图且 $n\geqslant 3$. 根据欧拉公式，G 的面数为 $m-n+2$. 因为 G 是简单图且 $n\geqslant 3$，其每个面至少由 3 条边围成，但每一条边是两个面的边界或在同一个面中两次出现，于是 $3(m-n+2)/2\leqslant m$，所以 $m\leqslant 3n-6$.

【例 7-16】 证明：K_5 不是平面图.

证 假设 K_5 是平面图，因为 K_5 是简单图且节点数 $n=5$，由推论 1 知，其边数为 $m\leqslant 3n-6=3\times 5-6=9$，而 $m=10$，矛盾.

类似于推论 1 的证明，有

推论 2 任意(n,m)简单连通平面图 G，若 G 不含 K_3 子图且 $n\geqslant 3$，则 $m\leqslant 2n-4$.

【例 7-17】 证明：$K_{3,3}$不是平面图.

证 假设 $K_{3,3}$是平面图，因为 $K_{3,3}$是简单图，节点数 $n=6$ 且不含 K_3 子图，由推论2 知，其边数为 $m\leqslant 2n-4=2\times 6-4=8$，而 $m=9$，矛盾.

下面的定理 7-11 是证明“五色定理”的关键.

【定理 7-11】 任何简单平面图必存在一个度数小于等于 5 的节点.

证 不妨设 $G=(V,E)$是(n,m)连通图且 $n\geqslant 3$. 若对于任意 $v\in V$ 均有 $\deg(v)\geqslant 6$，则有

$$\sum_{v\in V}\deg(v)\geqslant 6n \tag{1}$$

根据握手定理，有

$$\sum_{v\in V}\deg(v)=2m\leqslant 2(3n-6) \tag{2}$$

(1)与(2)矛盾，结论得证.

7.5.3 库拉托夫斯基定理

波兰数学家库拉托夫斯基（K. Kuratowski，1896—1980）于 1930 年给出了判定平面图的充要条件.

先介绍同胚的定义.

【定义 7-20】 若两个图是同构的，或者通过反复进行以下操作（如图 7-43 所示）使得它们同构，则称这两个图**同胚**(homeomorphism)：

(1) 移去一条边 v_1v_2，并增加一个节点 v 同时与 v_1，v_2 邻接.

(2) 删除一个度为 2 的节点 v，且在与 v 邻接的另外两个节点 v_1，v_2 之间连一条边.

【例 7-18】 证明：彼得森图的如下子图（如图 7-44 所示）G 同胚于 $K_{3,3}$.

证 显然.



图 7-43　　　　图 7-44

【定理 7-12】(Kuratowski，1930) 无向图 G 是平面图的充要条件是 G 无同胚于 K_5 和 $K_{3,3}$ 的子图.

库拉托夫斯基定理的证明是较困难的，可参见有关文献[16]. 根据库拉托夫斯基定理知，彼得森图不是平面图.

库拉托夫斯基定理给出了平面图的充要条件，但很难将其用于实际的平面图的判定. 在 1966 年，Lempel，Euler 和 Cederbaum 给出的“灌木生长算法”可以逐次完成平面图的嵌入，它是现代图论算法中十分直观、十分精彩的算法之一，而与之配套的 BFS 和 DFS 是很多图论算法的基础，它的基本思想是“走一步是一步，得进且进，行不通时再后退”.

7.5.4 平面图的对偶图

对平面图的面的研究可以转换为对其对偶图的节点的研究.

【定义 7-21】 设 G 是平面图，G 的**对偶图**(dual graph)G^* 构造如下：

(1) 在 G 的每个面内取一个点作为 G^* 的节点.

(2) 若 G 内的两个面有公共的边界 e，则在 G^* 中相应的两个节点之间连一条边 e^*，且使 e^* 与 e 相交一次而与 G 的其他边不相交. 若 e 是 G 的桥，则 e^* 为 G^* 的吊环. 若 e 是 G 的吊环，则 e^* 为 G^* 的桥.

如图 7-45 所示的对偶图为空心点虚线边所画的图.

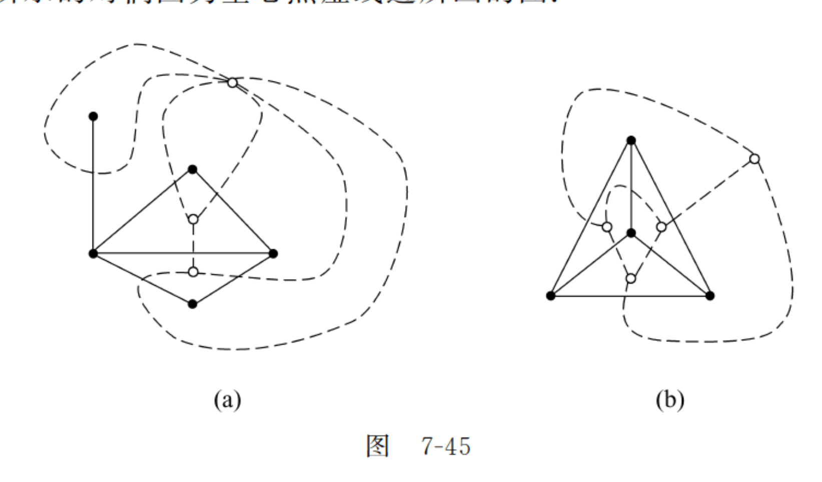


图 7-45

根据定义知，任意平面图的对偶图是平面图且是连通的. 设 G 是 (n,m) 平面图，有 r 个面，则 G^* 是 (r,m) 平面图，有 n 个面.

对于连通平面图 G，其对偶图为 G^*，这时 G^* 的对偶图 G^{**} 为 G 本身. 对于非连通平面图 G，G^{**} 可能与 G 不同构，如图 7-46 所示.

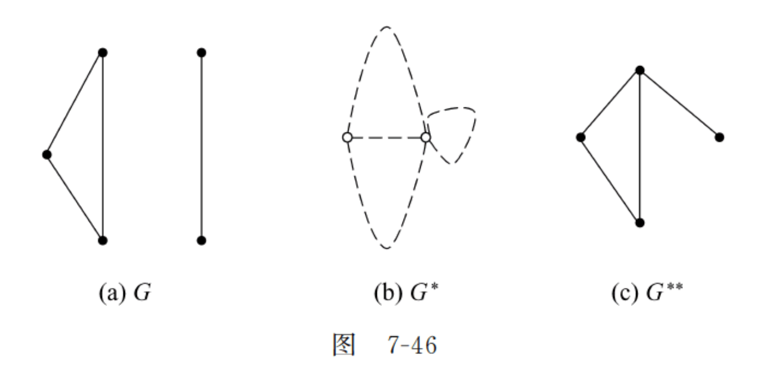


图 7-46

习 题 7.5

1. 证明：K_5 和 $K_{3,3}$ 都是极小非平面图.

2. 设 G 是 $n(n\geqslant 3)$ 阶极大平面图，试证明

(1) G 是连通图.

(2) G 的每个面都是三角形.

3. 边数 $m<30$ 的简单平面图 G，必存在节点 v 使得 $\deg(v)\leqslant 4$.

4. 设 G 是至少 11 个节点的简单图，则 G 或 $\overline{G}$ 不是平面图.

5. 利用欧拉公式证明：彼得森图是非平面图.

6. 证明：最小度 $\delta(G)\geqslant 3$ 的简单连通平面图 G 的边数不可能为 7.

7. 若 (n,m) 平面图的每个面至少由 $k(k\geqslant 3)$ 条边围成，则 $m\leqslant k(n-2)/(k-2)$.

8. 任意 (n,m) 平面图 G 的面数 $r=m-n+(w(G)+1)$，其中 $w(G)$ 是图 G 的连通分支数.

9. 任何 $n(\geqslant 3)$ 阶简单平面图 G 必存在 3 个度数小于等于 5 的节点.

10. 分别画出图 7-47(a)与图 7-47(b)的对偶图.

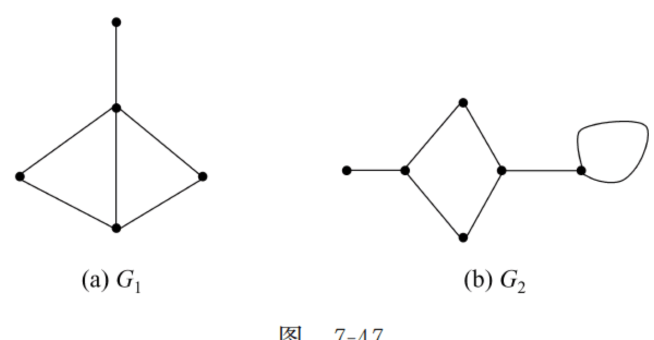


图 7-47

11. 给出例子说明，即使平面图 $G_1\cong G_2$，但 $G_1^*\cong G_2^*$ 不成立.

12. 设简单连通平面图 G 的节点数 $n=6$ 且边数 $m=12$，求 G 的面数 r 以及围每个面所需的边数.

13. 给出平面图 G 的对偶图 G^* 是欧拉图的充要条件.

14. 设平面图 G 有两个连通分支 K_3,K_4,问 G 的对偶图 G^* 是欧拉图还是哈密尔顿图?阐述理由.

15. 设平面图 G 有 r 个面,且每两个面均有公共边,求 r 的最大值.

16. 设 $n(n\geqslant 3)$阶无向图 G 是极大平面图,证明:G 的对偶图 G^* 是 3-正则图且 G^* 的边连通度 $\lambda(G^*)\geqslant 2$.

17. 设(n, m)图 G 是简单连通平面图,证明

(1) 若 $n\geqslant 3$,则 G 的面数 $r\leqslant 2n-4$.

(2) 若 G 的最小度 $\delta(G)=4$,则 G 中至少存在 6 个节点的度数小于等于 5.

18. 设(n, m)图 G 是简单平面图,其面数为 r,且 G 的最小度 $\delta(G)\geqslant 3$.

(1) 若 $r<12$,则 G 必存在一个至多 4 条边围成的面.

(2) 举例说明,若 $r=12$,则(1)中结论不成立.

7.6 平面图的面着色

1852 年,英国的一位大学生 F. 格思里(F. Guthrie)在给一张地图涂色时发现,要使有公共边的两个地方出现不同颜色,4 种颜色即可. 这就是著名的**四色猜想**(Four Color Conjecture,4CC).

F. Guthrie 将这个结论告诉了他的老师 De Morgan,一位当时非常有名的数学家. 由于 De Morgan 不知道该如何准确回答,便写信求教于 William Rowan Hamilton. 3 天后,Hamilton 回信说:"我不可能很快解决你的问题".

1879 年伦敦数学会会员 A. B. Kemple 给出了四色猜想的第一个证明,10 年后 P. J. Heawood 指出了 Kemple 证明过程中存在一个不可克服的漏洞,并沿用 Kemple 的方法证明了五色定理,即 5 种颜色足够.

在接下来的近 100 年里,为了攻克四色猜想,促进了图论以及图的网络理论的发展,它成了数学园地里会下金蛋的鹅. 在 1976 年,美国的 Kenneth Appel 和 Wolfgang Haken 与 John Koch 合作,在 Kemple 思想的基础上,借助于计算机用了 1260 个小时,用了 100 多亿次逻辑判断证明了"四色猜想",证明的关键技巧是继承了 Kemple 的"色交换技术",它开启了定理机器证明的新篇章,四色猜想变成四色定理了. 1999 年又给出了一些改进,缩短了计算机的运行时间.

尽管四色定理的证明没有得到完全承认,但至今为止还没有发现它的纯数学证明. 四色定理的简短证明可能有朝一日会被发现,也许出自一位天才的大学生之手.

本节主要内容是平面图的面着色问题,顺便介绍任意无向图的节点着色以及边着色等有关内容.

7.6.1 平面图的面着色定义

【定义 7-22】 设 G 是平面图,若对 G 的每个面涂上一种颜色且相邻的面出现不同的颜色,则称对该平面图的**面着色**(face coloring),所需颜色的最少种数称为**面着色数**(region chromatic number).

图 7-48(a)、图 7-48(b)和图 7-48(c)中各平面图的面着色数分别为 3，3，2.

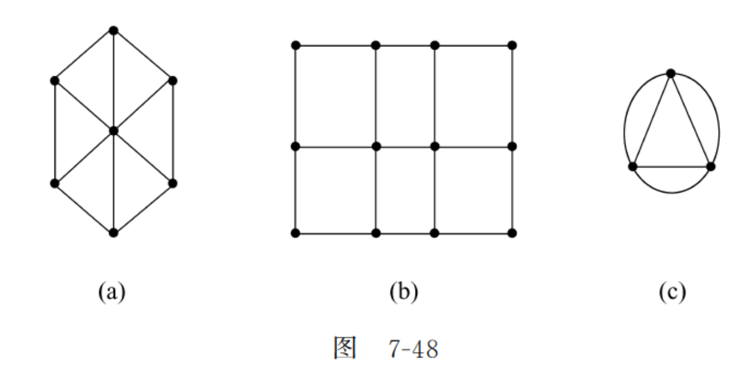


图　7-48

思考　你能给出一种平面图的面着色的算法及实现方案吗?

7.6.2　图的节点着色

1. 任意图的节点着色

【定义 7-23】　设 G 是任意无向图,若对 G 的每个节点涂上一种颜色且相邻的节点出现不同的颜色,则称对该图的**节点着色**(vertex coloring)，简称**着色**(coloring),所需颜色的最少种数称为节点着色数，简称**着色数**(chromatic number),记为 $\chi(G)$.

图 7-48(a)、图 7-48(b)和图 7-48(c)中各图的节点着色数分别为 3，2，3.

显然,$\chi(K_n)=n$.

容易证明

【定理 7-13】　设 G 是不含自环的图,则 $\chi(G)\leqslant\Delta(G)+1$.

证　(留作练习).

可以利用韦尔奇・鲍威尔(Welch Powell)算法对图 G 的节点着色,进而求出 $\chi(G)$的上界.

Welch Powell 算法:

(1) 将图 G 的节点按度数从大到小的顺序排列.

(2) 用第一种颜色对第一个节点着色,并且按照其余未着色节点顺序,对不邻接的每一个节点着上同样的颜色.

(3) 用第二种颜色对尚未着色的点重复(2),继续下去,直到所有的点都着色为止.

【例 7-19】　利用 Welch Powell 算法对如图 7-49 所示中的图 G 着色.

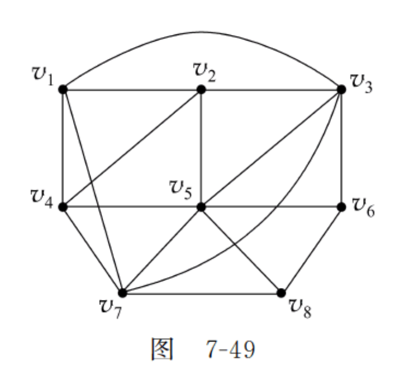


图　7-49

解　(1) 将图 G 的节点按度数从大到小的顺序排列为

$$v_5,v_3,v_7,v_1,v_2,v_4,v_6,v_8$$

(2) 用第一种颜色对 v_5 着色,并且按照顺序,对与 v_5 不邻接的节点 v_1 着上同样的颜色.

(3) 用第二种颜色对 v_3 着色,并且按照 v_7,v_2,v_4,v_6,v_8 顺序,对与 v_3 不邻接的节点 v_4 和 v_8 着上第二种颜色.

(4) 用第三种颜色对 v_7 着色,并且按照 v_2,v_6 顺序,对与 v_7 不邻接的节点 v_2 和 v_6 着上第三种颜色.

由此可知，$\chi(G)\leqslant 3$. 显然，$\chi(G)=3$.

2. 平面图的节点着色

平面图的节点着色与一般无向图的节点着色是相同的.

值得注意的是，平面图的面着色，可以转换为其对偶图(也是平面图)的节点着色. 于是，五色定理如下.

【定理 7-14】 设 G 是简单平面图，则 $\chi(G)\leqslant 5$.

证 对图 G 的节点数 n 归纳. 当 $n\leqslant 5$ 时结论显然. 假设对于 $n-1$ 阶简单平面图结论成立.

由 7.5 节定理 7-11 知，G 中存在一个节点 v 使得 $\deg(v)\leqslant 5$. 考虑 $G-\{v\}$. 由归纳假设有 $\chi(G-\{v\})\leqslant 5$.

若 $\deg(v)<5$，则与 v 邻接的节点个数 $\leqslant 4$，可对 v 着色.

若 $\deg(v)=5$，令与 v 邻接的节点分别为 v_1, v_2, v_3, v_4, v_5，它们分别着色 c_1, c_2, c_3, c_4, c_5. 设 W_1 为 $G-\{v\}$ 中着色为 c_1, c_3 的节点组成的集，W_2 为 $G-\{v\}$ 中着色为 c_2, c_4 的节点组成的集.

(1) 若 v_1, v_3 分别在 W_1 所导出子图的不同连通分支中，将 v_1 所在连通分支中的颜色 c_1, c_3 对调，不影响 $G-\{v\}$ 的着色，再对 v 着色 c_1，得图 G 的着色.

(2) 若 v_1, v_3 在 W_1 所导出子图的同一个连通分支中，则从 v_1 到 v_3 存在一条路 L，L 上的各点都着 c_1, c_3 色的. 路 L 与边 vv_1 和 vv_3 构成回路 C，它包围了 v_2 或 v_4，但不能同时包含，于是 v_2 和 v_4 分别属于节点集 W_2 所导出子图的两个连通分支中. 因此，在包含 v_2 的连通分支中，将颜色 c_2, c_4 对调，不影响 $G-\{v\}$ 的着色，再对 v 着色 c_2，得图 G 的着色.

7.6.3 任意图的边着色

【定义 7-24】 设 G 是任意无向图，若对 G 的每条边涂上一种颜色且相邻的边出现不同的颜色，则称对该图的**边着色**(edge coloring)，所需颜色的最少种数称为**边着色数**(edge-chromatic number).

图中的两条边相邻是指它们有公共的节点. 容易得出图 7-48(a)～图 7-48(c)中各图的边着色数分别为 6，4，6.

我们对图的边着色问题不做更深入讨论，最后对与拉姆塞(Ramsey)理论密切相关的图的边“涂色”的问题进行简单说明.

拉姆塞问题(Ramsey problem) 任给一群人，其中有 p 个人彼此认识或有 q 个人彼此不认识，这种人群至少多少人？

拉姆塞问题中的答案记为 $R(p,q)$.

【例 7-20】 证明：任意 6 个人中，有 3 个人彼此认识或有 3 个人彼此不认识.

证 用 6 个节点分别表示这 6 个人，可得六阶完全无向图 K_6. 若两个人认识，则在相应的两个节点所在的边上涂上红色，若两个人不认识，则在相应的两个节点所在的边上涂上蓝色.

对于任意的 K_6 的节点 v，因为 $\deg(v)=5$，与 v 关联的边有 5 条，当用红、蓝颜色去涂时，至少根据推广的鸽笼原理知，至少 $\left\lceil \frac{5}{2} \right\rceil=3$ 条边涂的是同一种颜色，不妨设 vv_1, vv_2, vv_3

是红色. 若 3 条边 v_1v_2,v_2v_3,v_1v_3 是红色,则存在红色 K_3,这意味着有 3 个人相互认识;若 v_1v_2,v_2v_3,v_1v_3 都是蓝色,则存在蓝色 K_3,这意味着有 3 个人相互不认识. 结论成立.

注意 在 5 个人的人群中,上述结论不成立. 只需要对 K_5 最外面的 5 条边涂成红色,里面的 5 条边涂成蓝色即可. 于是,$R(3,3)=6$(F. P. Ramsey, 1930).

已经知道的一些结果如下:

$$R(3,4)=9,\ R(3,5)=14,\ R(4,4)=18(1955)$$

$$R(3,6)=18(1964,\ 1966).\ R(3,7)=23(1968)$$

$$R(3,8)=28(1992).\ R(3,9)=36(1982).\ R(4,5)=25(1993)$$

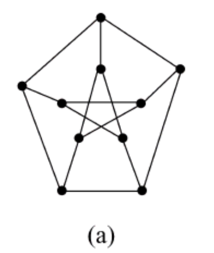
就 1993 年利用计算机得到的结果 $R(4,5)=25$ 来说,其计算量相当于一台标准计算机 11 年的计算量. 由此可见,由拉姆塞在 1928 年提出的求 $R(p,q)$ 的难题,是对数学科学和计算机科学的又一次极大挑战. 目前,可以先考虑计算 $R(5,5)$. 参见 http://mathworld.wolfram.com/RamseyNumber.html. 同时,可以采用上、下界逼近技巧求出 Ramsey 数.

习 题 7.6

1. 设 G 是不含桥的连通平面图,若 G 的面色数为 2,则 G 是欧拉图.

2. 证明:$\chi(K_n)=n$.

3. 分别求出如图 7-50 所示中各图的节点着色数和边着色数.



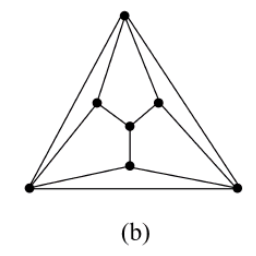
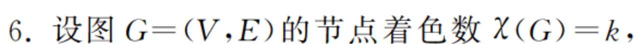


图 7-50

4. 设 G 是不含吊环的图,则 $\chi(G)\leqslant\Delta(G)+1$.

5. 设图 G 的节点着色数 $\chi(G)=k$,则 G 至少有 $k(k-1)/2$ 条边.



6. 设图 $G=(V,E)$ 的节点着色数 $\chi(G)=k$,且对于任意 $v\in V$,有 $\chi(G-v)<\chi(G)$,则 G 的最小度 $\delta(G)\geqslant k-1$.

7. 设 G 是简单图,若 G 的节点表示期末考试的科目,边表示关联的两节点所对应的科目不能在同一时间考试,问图 G 的节点着色的实际意义是什么?$\chi(G)$的实际意义是什么?

8. 用 C_{n-1} 表示有 $n-1$ 个节点的 $n-1$ 边形($n\geqslant4$). 在 C_{n-1} 内有放置一个节点并与 C_{n-1} 中所有节点邻接,这样得到的图称为 n 阶**轮图**,记为 W_n. 证明:W_n($n\geqslant4$)的边着色数为 $n-1$.

9. 证明:任意 9 个人中,有 3 个人相互认识或 4 个人相互不认识.

7.7 二部图匹配

在诸如人员分配、资源分配等问题的讨论中,经常涉及二部图及其匹配.

本节仅对简单无向图进行讨论.

7.7.1 二部图

【定义 7-25】 设 $G=(V,E)$是简单无向图,若 V 可划分为两部分 V_1 和 V_2,使得对于任

意 $e \in E$，都存在 $u \in V_1, v \in V_2$，使得 $e = uv = \{u, v\}$，则称 G 为**二部图**(bipartite graph)，V_1 和 V_2 称为**互补节点集**.

二部图又称为二分图或偶图. 例如图 7-51 所示都是二部图，它们是二部图的一般画法.

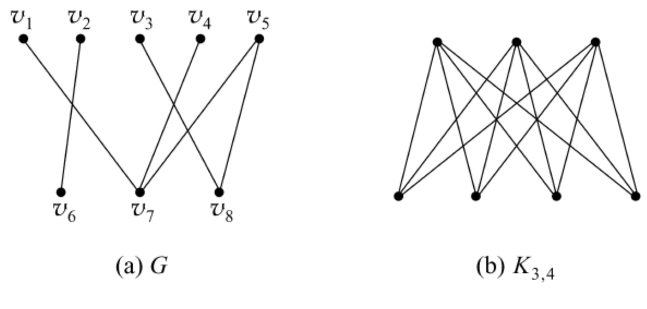


图 7-51

注意 二部图的互补节点集的划分不是唯一的. 例如在图 7-51(a) 中，可取 $V_1 = \{v_1, v_2, v_3, v_4, v_5\}$ 且 $V_2 = \{v_6, v_7, v_8\}$，也可取 $V_1 = \{v_1, v_3, v_4, v_5, v_6\}$ 且 $V_2 = \{v_2, v_7, v_8\}$.

设 G 为二部图，V_1 和 V_2 称为互补节点集. 若 V_1 中的所有节点与 V_2 的所有节点都邻接，则称 G 为**完全二部图**(complete bipartite graph)，记为 $K_{m,n}$，其中 $|V_1| = m$，$|V_2| = n$.

完全二部图 $K_{1,n}$ 称为**星状图**(star graph).

下面的定理给出了简单无向图是二部图的充要条件.

【定理 7-15】 设 $G = (V, E)$ 为阶数 $\geqslant 2$ 的简单连通无向图，则 G 是二部图的充要条件是 G 中任意回路的长度为偶数.

证 ($\Rightarrow$) 显然.

取 $v \in V$，令

$$V_1 = \{u \mid u \in V \text{ 且 } d(u, v) \text{ 是偶数}\}, \quad V_2 = V - V_1 \neq \varnothing$$

若存在边 $e \in E$，其关联的两个节点在同一个 $V_i (i = 1, 2)$ 中，则 G 中存在长度为奇数的回路，与已知矛盾. 于是，G 的任意边的两个端点，一个在 V_1 中，一个在 V_2 中. 故 G 是二部图.

由于在任意阶数 $\geqslant 2$ 无向树中不存在圈，其中任意回路的长度为偶数，因此任意无向树是二部图.

7.7.2 匹配

工作安排、资源分配、各种配对竞赛以及人员择偶等问题，实际上是匹配问题.

【定义 7-26】 设 $G = (V, E)$ 是简单无向图. 若 $\varnothing \neq M \subseteq E$ 且 M 中任何两条边都不相邻，则称 M 为 G 的一个**匹配**(matching)或**边独立集**(independent set of edges)，M 中每条边的两个节点在 M 中相配. 边数最多的匹配称为**最大匹配**(maximum matching)，其中的边数称为**匹配数**. 所有节点都与 M 中的某边关联的匹配称为**完美匹配**(perfect matching).

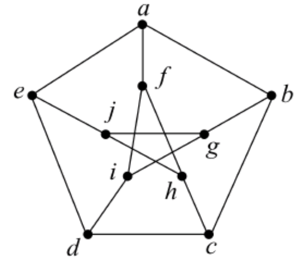


图 7-52

在图 7-52 所示的 Petersen 图 G 中，$\{ab, fh, id\}$ 和 $\{ab, fi, cd, hj\}$ 是 G 的一个匹配，$\{af, bg, ch, di, ej\}$ 是 G 的最大匹配，匹配数为 5，$\{af, bg, ch, di, ej\}$ 也是 G 的完美匹配.

对于简单无向图 $G = (V, E)$，令 $\varnothing \neq W \subseteq V$，若 W 中任意两个节点均不相邻，则称 W 为 G 的**点独立集**(independent set of nodes).

若 $G[W]$ 是完全图，则称 W 为 G 的**团**(clique).

在二部图 $G=(V,E)$ 中，V_1 和 V_2 为互补节点集. 若 M 为 G 的一个最大匹配且 $|M|=\min\{|V_1|,|V_2|\}$，则称 M 为 G 的一个**完备匹配**(complete matching). 当 $|V_1|\leqslant|V_2|$，也称 M 为 G 的一个从 V_1 到 V_2 的完备匹配.

1935 年 Hall 给出了判定二部图是否存在完备匹配的充要条件——“相异性条件”.

【定理 7-16】 (Hall, 1935) 设 $G=(V,E)$ 是二部图，V_1 和 V_2 是其互补节点集. G 中存在从 V_1 到 V_2 的完备匹配的充要条件是 V_1 中的任意 $k(k=1,2,\cdots,|V_1|)$ 个节点至少与 V_2 中的 k 个节点邻接.

匈牙利(Hungarian)算法(J. Edmonds, 1965)可用于求从 V_1 到 V_2 的完备匹配，参见有关文献[4].

根据 Hall 定理可得下面的定理.

【定理 7-17】 设 $G=(V,E)$ 是二部图，V_1 和 V_2 称为互补节点集. 若存在 $t\geqslant 1$，则使得如下“t 条件”成立：

(1) V_1 中的每个节点至少关联 t 条边.

(2) V_2 中的每个节点至多关联 t 条边，则 G 中存在从 V_1 到 V_2 的完备匹配.

证 由(1)，V_1 中的任意 $k(k=1,2,\cdots,|V_1|)$ 个节点至少与 kt 条边关联. 再由(2)，这些边至少与 V_2 中的 k 个节点邻接. 由 Hall 定理即证.

下述定理给出了任意简单无向图存在完美匹配的充要条件.

【定理 7-18】 (Tutte) 图 $G=(V,E)$ 有完美匹配的充要条件是对于任意 $W\subseteq V$ 均有 $O(G-W)\leqslant|W|$，其中 $O(G-W)$ 表示含奇数个节点的连通分支数.

习　题　7.7

1. 判断如图 7-53 所示是否为二部图. 若是二部图，求出其互补节点集.

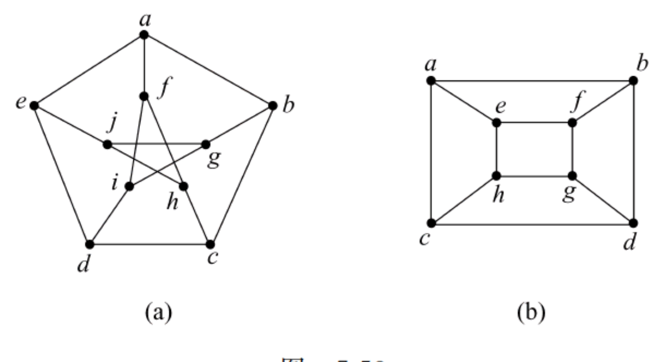


图　7-53

2. 捕获 6 名间谍 a,b,c,d,e,f，其中 a 会汉语、法语和日语；b 会德语、日语和俄语；c 会英语和法语；d 会汉语和西班牙语；e 会英语和德语；f 会俄语和西班牙语. 如将这 6 人用两个房间监禁，是否可以使得在同一房间里的任意两人不能相互直接交谈？

3. 有 6 位老师：张、王、李、赵、孙、周，要安排他们去教 6 门课：数学、化学、物理、语文、英语和计算机. 张老师可教数学、计算机和英语；王老师可教英语和语文；李老师可教数学和物理；赵老师只能教化学；孙老师可教物理和计算机；周老师可教数学和物理. 问怎样安排课

程才能使得每门课都有人教，每个人都只教一门课?

4．举例说明，满足"相异性条件"的二部图，不一定存在一个 $t\geqslant 1$ 使其满足"t 条件".

5．某年级共开设了7门课，有7位教师承担．已知每位教师都可以担任其中的3门课．他们将自己能担任的课上报教务处后，教务员发现每门课都恰有3位教师能承担．问教务员能否安排这7位教师每人担任1门课，且每门课都有人承担．(提示：利用 t 条件)

6．证明：阶数大于等于2的简单无向图 G 是二部图当且仅当 $\chi(G)\leqslant 2$.

7．证明：无向树至多有一个完美匹配.

8．利用 Tutte 定理证明：若 n 阶图 G 是 $k-1$ 边连通的 k 正则图，且 n 是偶数，则 G 存在完美匹配.

本章小结

1．欧拉图

设 $G=(V,E)$ 是任意图，G 中经过所有边一次且仅一次的路称为欧拉轨迹，G 中经过所有边一次且仅一次的回路称为欧拉回路，存在欧拉回路的图称为欧拉图.

欧拉定理　设 G 是连通无向图，则 G 是欧拉图的充要条件是 G 的每节点度数为偶数.

中国邮递员问题　边赋权的图中在添加平行边后求最短欧拉回路的问题.

掌握与欧拉图有关的3个概念和欧拉定理，理解其他几个结论，了解中国邮递员问题.

2．哈密尔顿图

设 $G=(V,E)$ 是任意图，G 中经过所有节点一次且仅一次的路径称为哈密尔顿路径，G 中经过所有节点一次且仅一次(除起点重复一次外)的圈称为哈密尔顿回路，存在哈密尔顿回路的图称为哈密尔顿图.

定理(Ore，1960)设 $G=(V,E)$ 是 $n(n\geqslant 3)$ 阶简单无向图，若对于任意的不相邻节点 u，v 有

$$\deg(u)+\deg(v)\geqslant n,$$

则 G 是哈密尔顿图.

旅行商问题(TSP)　在边赋权图中，找出一条权最小的哈密尔顿回路.

掌握与哈密尔顿有关的3个概念和 Ore 定理，理解其他几个结论，了解旅行商问题.

3．无向树

不含有圈的连通无向图称为无向树.

定理　以下关于无向 (n,m) 图 G 的6个命题等价.

(a) G 是一棵无向树.

(b) G 不含有圈且 $m=n-1$.

(c) G 连通且 $m=n-1$.

(d) G 不含有圈但增加一条新边后得到一个且仅一个圈.

(e) G 连通但删除任意一条边后便不连通.

(f) G 的每一对节点有且仅有一条路径.

设 $G=(V,E)$ 是无向图，是无向树的生成子图 T 称为 G 的生成树．无向图 G 存在生成

树的充要条件是 G 是连通图.

设 G 是边赋权的连通无向图,G 中权最小的生成树称为最小生成树. 理解求最小生成树的克鲁斯卡尔避圈法.

熟练掌握无向树的定义和性质，理解生成树和最小生成树并能运用克鲁斯卡尔算法求出最小生成树.

4. 有向树

了解有向树的定义：有向图 $G=(V,E)$,在不考虑边的方向时是一棵无向树,则该有向图称为有向树.

一棵有向树,若恰有一个节点入度为 0,而其余节点入度均为 1,则该有向树称为根树. 要求掌握根树的定义，了解树根、树叶、分支节点、父节点、子节点、子根树、高度(深度)等有关概念.

最大出度为 m 的根树称为 m 叉树. 设 $G=(V,E)$是一棵 m 叉树,若 G 的每一片树叶上都赋予一个非负实数,则称 G 为叶赋权 m 叉树. 理解求最优二叉树赫夫曼算法.

对同一个节点的所有儿子节点规定先后顺序的根树就是有序树.

对同一个节点的所有儿子节点规定左右位置的有序二叉树称为定位二叉树.

理解 m 叉树、有序树和定位二叉树概念，了解左右儿子、赫夫曼编码、遍历方式和有序森林到定位二叉树的转换.

5. 平面图

设 G 是无向图,若可将 G 画在一个平面上,同时使得任意两条边在非节点处不相交,则称 G 为平面图. 两个重要的非平面图：(1)K_5,(2)$K_{3,3}$.

设 G 是平面图,由 G 的若干条边所围成的连通区域称为图 G 的面.

欧拉公式 任意(n,m)连通平面图 G 的面数 $r=m-n+2$.

定理 任何简单平面图必存在一个度数$\leqslant 5$ 的节点.

掌握平面图及其面的定义和欧拉公式，能得出欧拉公式的推论并证明上述定理,了解库拉托夫斯基定理和平面图的对偶图.

6. 平面图的面着色

理解平面图的面着色(数)、任意无向图的节点着色(数)和边着色(数)，了解五色定理，能解决简单的拉姆塞问题，如 $R(3, 3) = 6$.

五色定理 设 G 是简单平面图,则 $\chi(G)\leqslant 5$.

拉姆塞问题 任给一群人,其中有 p 个人彼此认识或有 q 个人彼此不认识,这个人群至少有 $R(p,q)$人.

7. 二部图及其匹配

若简单无向图 $G=(V,E)$的节点集 V 可划分为两部分 V_1 和 V_2,使得对于任意 $e\in E$,都存在 $u\in V_1$,$v\in V_2$,使得 $e=uv=\{u, v\}$,则称 G 为二部图.

定理 设 G 为阶数$\geqslant 2$ 的简单连通无向图,则 G 是二部图的充要条件是 G 中任意回路的长度为偶数.

理解二部图的概念和有关结论、完全二部图 $K_{m,n}$，了解互补节点集、匹配(边独立集)、最大匹配、匹配数、完美匹配、点独立集、团、完备匹配等有关概念.

第8章 组合计数

我们知道，离散数学研究离散对象. 组合计数，简称计数(counting)就是计算满足一定条件的离散对象的安置方式的数目.

对于给定离散对象的安置方式，要考虑其存在性问题、计数问题、构造方法、最优化问题，这些是组合数学研究的全部内容(参见文献[6]). 组合数学发源于数学消遣和数学游戏，其研究历史可追溯到公元前2200年中国的大禹治水时代，从洛河中浮出的神龟背部上出现的三阶幻方开始，该方阵的每一行、每一列以及两条对角线的3个数字之和都等于15，其研究方兴未艾.

计算机科学是研究算法的一门科学，组合计数是算法分析与设计的基础，它对于分析算法的时间复杂度和空间复杂度是至关重要的. 当然，组合计数在诸多领域的很多问题的讨论中也经常用到. 从儿时的数"数"也略知组合计数的重要性.

本章主要讨论组合计数的基本计数技巧和方法，包括计数原理、排列组合、二项式定理、生成函数与递归关系等内容，它们都与集合、映射、运算和关系密切联系.

8.1 计数原理、排列组合与二项式定理

8.1.1 计数原理

计数原理有加法原理和乘法原理，它们是研究计数的基础.

加法原理(addition principle) 若事件 A_1 有 m_1 种不同选取方式，事件 A_2 有 m_2 种不同选取方式，……，事件 A_k 有 m_k 种不同选取方式，在这 k 个事件之间没有共同的选取方式时，则这 k 个事件之一发生有 $m_1+m_2+\cdots+m_k$ 种不同选取方式.

例如，假设一个班有 m_1 个男生，有 m_2 个女生，根据加法原理知，该班有 m_1+m_2 个同学. 若将计数的元素划分成若干个不同的类，先分类计数，再相加，这种方法称为分类处理，见图8-1(a).

乘法原理(multiplication principle) 若事件 A_1 有 m_1 种不同选取方式，事件 A_2 有 m_2 种不同选取方式，……，事件 A_k 有 m_k 种不同选取方式，则这 k 个事件依次发生有 $m_1m_2\cdots m_k$ 种不同选取方式.

例如，假设从 A 到 B 有 m_1 条线路，从 B 到 C 有 m_2 条线路，那么根据乘法原理知，从 A 先到 B 紧接着再从 B 到 C 就有 m_1m_2 条线路. 若计数时需要分成独立的几步才能完成，先分别计算每一步的选取方式，再相乘，这种方法称为分步处理，见图8-1(b).

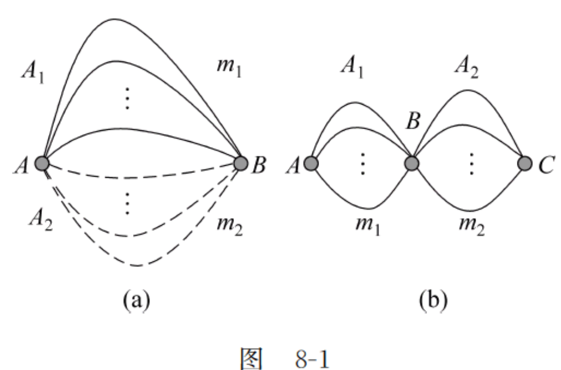


图 8-1

在计数过程中，分类处理和分步处理可能会

嵌套使用.

8.1.2 排列

1. n 个元素的 r-排列

从 n 个不同的元素中,取 r 个出来按顺序排列,就是 n 个元素的 **r-排列**(permutation),其排列个数记为 P_n^r 或 $P(n, r)$.

注意到 $n!=n(n-1)\cdots 3\cdot 2\cdot 1$. 随着 n 的增大,$n!$ 呈指数增长. Stirling 给出的近似公式为

$$n! \approx \sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n.$$

随着 n 的增大,二者的相对误差趋于 0:

$$\lim_{n\to\infty}\frac{n!}{\sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n}=0,$$

而绝对误差趋于无穷大:

$$\lim_{n\to\infty}\left[n!-\sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n\right]=+\infty.$$

利用乘法原理有下述结论.

【定理 8-1】 对于任意 $r\leqslant n$,有 $P_n^r=n(n-1)\cdots(n-r+1)=\dfrac{n!}{(n-r)!}$.

显然,n 个元素的全排列个数为 $n!$. 约定 $P_n^0=1$.

2. n 个元素的 r-圆排列

实际上,n 个元素的 r-排列是线排列. 如果从 n 个不同的元素中,取 r 个出来按顺序排列成一个圆,就是 n 个元素的 **r-圆排列**(circular permutation),这样的排列个数记为 $\odot P_n^r$ 或 $\odot P(n, r)$. 注意圆排列只与相对位置有关,例如图 8-2(a)和图 8-2(b)中的圆排列是相同的.

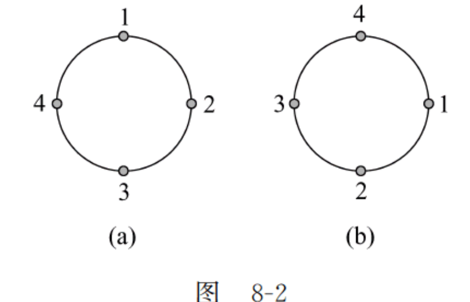


图 8-2

显然,上面的圆排列可以得到 1234,2341,3412 和 4123 四个线排列. 一般地,一个 r-圆排列可以得到 r 个 r-排列,于是

$$\odot P_n^r=\frac{P_n^r}{r}.$$

3. n 个元素的 r-可重排列

前面所讨论的排列中要求没有重复元素. 如果从 n 个不同的元素中,可重复取 r 个元素按顺序排列,就是 n 个元素的 **r-可重排列**(permutation with repetition),这样的排列个数记为 U_n^r 或 $U(n, r)$.

可以这样理解 r-可重排列:先从 n 个元素中任取一个元素出来排在第一位置,有 n 种选取方式. 将其放回后,再任意取一个元素出来排在第二位置,也有 n 种选取方式. 这样一直进行下去,直到有 r 个元素排列为止. 因此,根据乘法原理有

$$U_n^r=n^r.$$

4. 有重复元素的全排列

【定理 8-2】 设 $A_1, A_2, \cdots, A_k$ 是 k 个不同元素，现有 n_i 个 A_i 元素($i=1,2,\cdots,k, n_1+n_2+\cdots+n_k=n$)，即 $A=\{n_1 \cdot A_1, n_2 \cdot A_2, \cdots, n_k \cdot A_k\}$，则这 n 个元素的全排列个数为

$$\frac{n!}{n_1! n_2! \cdots n_k!}.$$

证 记这 n 个可重元素的全排列个数为 N. 将 n_i 个 A_i 元素看作不同的元素 $A_i^1, A_i^2, \cdots, A_i^{n_i}$ ($i=1,2,\cdots,k$)，于是得到 $n_1+n_2+\cdots+n_k=n$ 个不同元素，其全排列个数为 $n!$. 由于 n_i 个不同的元素 $A_i^1, A_i^2, \cdots, A_i^{n_i}$ 的全排列个数为 $n_i!$ ($i=1,2,\cdots,k$)，于是所给 n 个可重元素的一个全排列可以得到 $n_1!\ n_2!\ \cdots n_k!$ 个 n 个不同元素的全排列，根据乘法原理知 $N \cdot n_1!\ n_2!\ \cdots n_k! = n!$，进而

$$N = \frac{n!}{n_1! n_2! \cdots n_k!}.$$

8.1.3 组合

1. *n* 个元素的 *r*-组合

从 n 个不同的元素中，取 r 个出来放成一堆而不考虑其顺序，就是 n 个元素的 ***r*-组合**(combination)，其组合个数记为 C_n^r 或 $\binom{n}{r}$ 或 $C(n, r)$.

上面的三个组合个数的记号都是标准的，但 C_n^r 和 $\binom{n}{r}$ 容易混淆.

为了方便，约定当 $r>n$ 时，$C_n^r=0$；同时约定 $C_n^0=1, C_0^0=1$. 由于一个 r-组合可以得到 $r!$ 个 r-排列，根据乘法原理有下述结论.

【定理 8-3】 $C_n^r = \dfrac{P_n^r}{r!} = \dfrac{n(n-1)\cdots(n-r+1)}{r!} = \dfrac{n!}{(n-r)!\ r!}$.

2. *n* 个元素的 *r*-可重组合

如果从 n 个不同的元素中，可重复地取 r 个元素而不考虑其顺序，就是 n 个元素的 ***r*-可重组合**(combination with repetition)，这样的组合个数记为 F_n^r 或 $F(n, r)$.

【定理 8-4】 $F_n^r = C_{n+r-1}^r$.

证(Euler 证法) 不妨设 n 个不同元素分别为 $1,2,\cdots,n$. 可重复选取的 r 个元素为 $c_1, c_2, \cdots, c_r$，可设 $c_1 \leqslant c_2 \leqslant \cdots \leqslant c_r$. 记 $d_1=c_1, d_2=c_2+1, \cdots, d_r=c_r+(r-1)$，于是得到另外一个组合 $d_1, d_2, \cdots, d_r$. 显然 $f: c_i \to d_i, i=1,2,\cdots,r$ 是 $\{c_1, c_2, \cdots, c_r\}$ 构成集合到 $\{d_1, d_2, \cdots, d_r\}$ 构成集合的一一对应，于是组合 $c_1, c_2, \cdots, c_r$ 的个数与组合 $d_1, d_2, \cdots, d_r$ 的个数相同. 而组合 $d_1, d_2, \cdots, d_r$ 是在 $1,2,\cdots,n,n+1,\cdots,n+(r-1)$ 这 $n+r-1$ 个不同的元素的 r-组合，其个数为 C_{n+r-1}^r.

说明 一一对应是组合计数常用的解题技巧之一.

容易证明，n 个元素的 r-可重组合个数与不定方程 $x_1+x_2+\cdots+x_n=r$ 的非负整数解的个数相同. 利用这一点，可以证明：若 n 个元素的 r-可重组合中每个元素至少出现一次，则 $r \geqslant n$ 且这样的组合个数为 C_{r-1}^{n-1}.

【例 8-1】 从为数众多的一元币、五元币、十元币、五十元币和一百元币中选取 6 张出来，有多少种选取方式？

解　根据题意,就是从5个不同的元素中,可重复地取6个元素而不考虑其顺序的6-可重组合,其组合个数为

$$F_5^6=C_{5+6-1}^6=C_{10}^6=\frac{P_{10}^6}{6!}=\frac{10\times9\times8\times7\times6\times5}{6\times5\times4\times3\times2\times1}=210.$$

与组合 C_n^r 有关的恒等式有近1000个,下面是常用的三个组合恒等式,可采用组合的计算公式定理8-3加以证明,也可以根据组合的意义进行"组合证明".

(1) 对称公式 $C_n^r=C_n^{n-r}$.

(2) 加法公式 $C_n^r=C_{n-1}^r+C_{n-1}^{r-1}$.

(3) 移进移出公式 $C_n^r=\frac{n}{r}C_{n-1}^{r-1}$.

8.1.4　二项式定理

与组合密切相关的是下述二项式定理.

【定理8-5】(二项式定理)　设 n 为正整数,则对于任意 x 和 y,有

$$(x+y)^n=\sum_{r=0}^{n}C_n^r x^r y^{n-r}.$$

证　因为 $(x+y)^n=\overbrace{(x+y)(x+y)\cdots(x+y)}^{n}$,对于任意 $r(0\leqslant r\leqslant n)$,项 x^ry^{n-r} 就是在 r 个 $(x+y)$ 中都取 x,而在 $n-r$ 个 $(x+y)$ 中都取 y,作乘积得到的.于是 x^ry^{n-r} 的系数就是上述选法的个数,即 n 个元素的 r-组合数 C_n^r.

正因为这样,组合数 C_n^r 又称为**二项式系数**.根据二项式定理,有

$$(1+x)^n=\sum_{r=0}^{n}C_n^r x^r=1+C_n^1x+C_n^2x^2+\cdots+C_n^nx^n,$$

$$2^n=(1+1)^n=\sum_{r=0}^{n}C_n^r=C_n^0+C_n^1+\cdots+C_n^n.$$

思考　将所有 n 个元素的 r-排列和 r-组合列举出来的方法.

习　题　8.1

1. 将 A,B,C,D 这4个人分成两个组,有多少种不同的分组方法?

2. 求万位数字不是9和8且各位数字互异的五位数的个数.

3. 由 n 个不同元素 $A_1,A_2,\cdots,A_n$ 作成的 A_1,A_2 不相邻的全排列个数有多少?

4. 5男5女圆桌交替就座的方式有多少种?

5. 在平面上15个点,且任意3个点都不在同一条直线上,通过这些点可以确定多少条不同直线?可以得到多少个位置不同的三角形?

6. 证明:$C_n^r=C_{n-1}^r+C_{n-1}^{r-1}$.

7. 使用组合数 $C_n^r=\frac{n!}{r!\ (n-r)!}$ 证明定理8-2.

8.2 生成函数

前面从计数的加法原理和乘法原理出发,介绍了排列组合的概念以及一些计算其个数的公式.

生成函数(generating function)又称为母函数,它是解决满足一定要求的排列组合计数问题的一种重要工具,也是求解递归关系的一种工具.

利用生成函数解决计数问题的基本思想就是将要计算的个数 $a_r = f(r)$ 转化为一个关于 x 的函数,通过对 x^r 或$\frac{x^r}{r!}$的系数的讨论得出结论($r=0, 1, 2, \cdots$).

8.2.1 组合计数生成函数

【定义 8-1】 对于数列 $a_0, a_1, \cdots, a_r, \cdots$,**其组合计数生成函数**(ordinary generating function)为

$$G(x) = a_0 + a_1 x + \cdots + a_r x^r + \cdots = \sum_{r=0}^{\infty} a_r x^r.$$

在高等数学中,无穷多个函数相加称为函数项级数. 由于 $\sum_{r=0}^{\infty} a_r x^r$ 中的每个函数都是幂函数,所以 $\sum_{r=0}^{\infty} a_r x^r$ 称为幂级数.

设 n 个元素的 r-组合个数为 a_r, $r=0, 1, 2, \cdots$. 显然,有 $a_r = \begin{cases} 1, & r=0 \\ C_n^r, & r \leqslant n \\ 0, & r > n \end{cases}$,其组合计数生成函数为

$$\begin{aligned} & 1 + C_n^1 x + C_n^2 x^2 + \cdots + C_n^n x^n \\ = & (1+x)^n = \overbrace{(1+x)(1+x)\cdots(1+x)}^{n}. \end{aligned}$$

于是,a_r 就是其组合计数生成函数 $\sum_{r=0}^{\infty} a_r x^r$ 中 x^r 的系数且

$$\sum_{r=0}^{\infty} a_r x^r = \overbrace{(1+x)(1+x)\cdots(1+x)}^{n} = (1+x)^n.$$

实际上,$\overbrace{(1+x)(1+x)\cdots(1+x)}^{n}$中第 i 个$(1+x)$可理解为 n 个元素中的第 i 个元素,其中的“1”表示在组合中不取第 i 个元素,“x”表示在组合中选取了第 i 元素($i=1, 2, \cdots, n$).

设 n 个元素的 r-可重组合个数为 a_r, $r=0, 1, 2, \cdots$. 显然,有 $a_r = C_{n+r-1}^r$,特别地 $a_0 = 1$. 现考虑$\overbrace{(1+x+x^2+\cdots)(1+x+x^2+\cdots)\cdots(1+x+x^2+\cdots)}^{n}$,其展开式中 x^r 来源于第一个括号$(1+x+x^2+\cdots)$中的 x^{m_1},第二个括号$(1+x+x^2+\cdots)$中的 x^{m_2},$\cdots$,第 n 个括号$(1+x+x^2+\cdots)$中的 x^{m_n} 的乘积,即 $x^{m_1} x^{m_2} \cdots x^{m_n} = x^r$,这时 $m_1 + m_2 + \cdots + m_n = r$, $m_i \geqslant 0$, $i=1$,

2，…，n. 该不定方程的非负整数解的个数即为 $a_r=C_{n+r-1}^r$. 换句话说，有

$$\sum_{r=0}^{\infty} a_r x^r = \overbrace{(1+x+x^2+\cdots)\cdots(1+x+x^2+\cdots)}^{n} = (1+x+x^2+\cdots)^n.$$

因此，上式右边展开式中 x^r 的系数就是 a_r.

实际上，$\overbrace{(1+x+x^2+\cdots)(1+x+x^2+\cdots)\cdots(1+x+x^2+\cdots)}^{n}$中的第 i 个$(1+x+x^2+\cdots)$可理解为 n 个元素中的第 i 个元素，其中的“1”表示在组合中不取第 i 个元素，“x”表示在组合中第 i 个元素取一次，“x^2”表示在组合中第 i 个元素取了 2 次，“x^3”表示在组合中第 i 个元素取了 3 次，…，$(i=1, 2, \cdots, n)$.

上述思想还可以推广，例如在组合计数生成函数中出现乘积项(x^2+x^4)，则表示对应的元素可取 2 次或 4 次.

同时，从上面的讨论还可以知道，所有的生成函数是一个“形式幂级数”，我们并不十分关心该幂级数的收敛域.

对于生成函数，可以像高等数学中函数项级数一样进行加、减、乘、除、微分和积分等运算，参见高等数学相关教材. 研究表明，高等数学中给出的常见函数的幂级数展开所得到的有关结论，在形式幂级数中仍然成立. 例如下面是 3 个常用的形式幂级数如下(需要记住)：

(1) $\dfrac{1}{1-x}=1+x+x^2+\cdots$.

(2) $(1+x)^m=1+mx+\dfrac{m(m-1)}{2!}x^2+\cdots+\dfrac{m(m-1)\cdots(m-n+1)}{n!}x^n+\cdots$，($m$ 为实数).

(3) $e^x=1+x+\dfrac{1}{2!}x^2+\dfrac{1}{3!}x^3+\cdots$.

下面通过例子说明如何利用组合计数生成函数解决一般的组合计数问题.

【例 8-2】 一口袋中有 5 个红球，3 个黄球，绿、白、黑球可任意多提供. 现从中取 3 个球，有多少种选取方式?

解 设取 r 个球的方法有 a_r 种($r=0,1,2,\cdots$)，则组合计数生成函数

$$\begin{aligned}G(x)&=a_0+a_1x+a_2x^2+a_3x^3+\cdots\\&=(1+x+x^2+x^3+x^4+x^5)(1+x+x^2+x^3)(1+x+x^2+\cdots)^3\\&=(1+2x+3x^2+4x^3+4x^4+4x^5+3x^6+2x^7+x^8)\left(\frac{1}{1-x}\right)^3,\end{aligned}$$

其展开式中 x^3 的系数就是要计算的选取方式 a_3. 由于 $a_3=\dfrac{1}{3!}G^{(3)}(0)$，经计算知 $G^{(3)}(0)=210$，所以 $a_3=35$.

在上例中，因为要计算的是取 3 个球的方式数，可取 $G(x)=(1+x^2+x^3)^5$ 或 $G(x)=(1+x^2+x^3+\cdots)^5=(1-x)^{-5}$.

【例 8-3】 现有 $2n$ 个 A，$2n$ 个 B，$2n$ 个 C，求从它们中选出 $3n$ 个字母的方式数.

解 设取 r 个字母的方法有 a_r 种($r=0,1,2,\cdots$)，则组合计数生成函数

$$G(x)=a_0+a_1x+a_2x^2+a_3x^3+\cdots$$

$$
\begin{aligned}
&= (1+x+x^2+\cdots+x^{2n})^3 = \left(\frac{1-x^{2n+1}}{1-x}\right)^3 \\
&= (1-x^{2n+1})^3(1+(-x))^{-3} \\
&= (1-3x^{2n+1}+3x^{4n+2}-x^{6n+3})\left(1+\sum_{k=0}^{\infty}\frac{(-3)(-4)\cdots(-k-2)}{k!}(-x)^k\right) \\
&= (1-3x^{2n+1}+3x^{4n+2}-x^{6n+3})\left(1+\sum_{k=0}^{\infty}\frac{3\cdot 4\cdots(k+2)}{k!}x^k\right) \\
&= (1-3x^{2n+1}+3x^{4n+2}-x^{6n+3})\sum_{k=0}^{\infty}C_{k+2}^2 x^k.
\end{aligned}
$$

于是,上式中 x^{3n}的系数为 $C_{3n+2}^2-3C_{n+1}^2$.

8.2.2 排列计数生成函数

【定义 8-2】 对于数列 $a_0,a_1,\cdots,a_r,\cdots$,其**排列计数生成函数**(exponential generating function)为

$$
E(x)=a_0+a_1x+a_2\frac{x^2}{2!}+\cdots+a_r\frac{x^r}{r!}+\cdots=\sum_{r=0}^{\infty}a_r\frac{x^r}{r!},
$$

这时,排列个数 a_r 是$\frac{x^r}{r!}$的系数.

可以证明下述定理.

【定理 8-6】 设 $A_1,A_2,\cdots,A_k$ 是 k 个不同元素,现有 n_i 个 A_i 元素($i=1,2,\cdots,k,n_1+n_2+\cdots+n_k=n$),则在这 n 个元素中任取 r 个元素的排列个数为 a_r,其排列计数生成函数为

$$
\begin{aligned}
&a_0+a_1x+a_2\frac{x^2}{2!}+\cdots+a_r\frac{x^r}{r!}+\cdots \\
=&\left(1+x+\frac{x^2}{2!}+\cdots+\frac{x^{n_1}}{n_1!}\right)\left(1+x+\frac{x^2}{2!}+\cdots+\frac{x^{n_2}}{n_2!}\right)\cdots\left(1+x+\frac{x^2}{2!}+\cdots+\frac{x^{n_k}}{n_k!}\right).
\end{aligned}
$$

实际上,上式右边的第 i 个括号$\left(1+x+\frac{x^2}{2!}+\cdots+\frac{x^{n_i}}{n_i!}\right)$表示第 i 个元素,其中的 1 表示不取第 i 个元素,x 表示第 i 个元素取了一次用来排列,$\frac{x^2}{2!}$表示第 i 个元素取了两次用来排列,$\cdots$,$\frac{x^{n_i}}{n_i!}$表示第 i 个元素取了 n_i 次用来排列,当然第 i 个元素最多取 n_i 次($i=1,2,\cdots,k$).

类似地,若一个元素在排列中至少取 2 次,至多取 5 次,则在排列计数生成函数中应出现乘积项$\left(\frac{x^2}{2!}+\frac{x^3}{3!}+\frac{x^4}{4!}+\frac{x^5}{5!}\right)$. 利用该思想可以解决很多的排列计数问题.

【例 8-4】 用 0,1,2,3,4 五个数字,求可组成六位数的个数,其中 0 恰出现 1 次,1 出现 2 次或 3 次,2 不出现或出现 1 次,3 没有限制,4 出现奇数次.

解 先计算不出现 0 的满足其余条件的五位数个数.

设不出现 0 的满足其余条件的 r 位数个数为 a_r,则排列计数生成函数

$$
E(x)=\left(\frac{x^2}{2!}+\frac{x^3}{3!}\right)(1+x)\left(1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\cdots\right)\left(x+\frac{x^3}{3!}+\frac{x^5}{5!}+\cdots\right)
$$

$$=\left(\frac{x^2}{2}+\frac{x^3}{6}\right)(1+x)\mathrm{e}^x\cdot\frac{1}{2}(\mathrm{e}^x-\mathrm{e}^{-x})$$
$$=\left(\frac{x^2}{4}+\frac{2x^3}{6}+\frac{x^4}{12}\right)(\mathrm{e}^{2x}-1)$$
$$=\left(\frac{x^2}{4}+\frac{2x^3}{6}+\frac{x^4}{12}\right)\left(\sum_{r=0}^{\infty}\frac{(2x)^r}{r!}-1\right).$$

因此,x^5 的系数为

$$\frac{1}{4}\cdot\frac{2^3}{3!}+\frac{1}{3}\cdot\frac{2^2}{2!}+\frac{1}{12}\cdot\frac{2^1}{1!}=\frac{7}{6},$$

进而$\frac{x^5}{5!}$的系数为$\frac{7}{6}\cdot 5!=140$,即 $a_5=140$.

由于在满足要求的六位数中,0 恰出现一次,而由所求出的每个五位数可得到 5 个不同的六位数,如由 12134 可得到 121340,121034,121304,120134,102134,故满足要求的六位数有 $140\times5=700$.

【例 8-5】 将 n 个点排成一条直线,用红、白、黑 3 种颜色对其任意涂色,要求同色点为偶数(包括 0),有多少种涂法?

解 这是一个排列问题,设排成一行的 r 个点满足要求的涂法有 a_r 种,$r=0,1,2,\cdots$,则排列计数生成函数

$$E(x)=\left(1+\frac{x^2}{2!}+\frac{x^4}{4!}+\cdots\right)^3,$$

其中每一个括号代表一种颜色.

$$E(x)=\left(\frac{\mathrm{e}^x+\mathrm{e}^{-x}}{2}\right)^3$$
$$=\frac{\mathrm{e}^{3x}+3\mathrm{e}^x+3\mathrm{e}^{-x}+\mathrm{e}^{-3x}}{8}$$
$$=\sum_{n=0}^{\infty}\frac{1}{8}(3^n+3+3(-1)^n+(-3)^n)\frac{1}{n!}x^n,$$

于是

$$a_n=\frac{1}{8}(3^n+3+3(-1)^n+(-3)^n).$$

习 题 8.2

1. 分别写出由数列 $1,-1,\frac{1}{2!},-\frac{1}{3!},\frac{1}{4!},-\frac{1}{5!},\cdots$得出的组合计数生成函数和排列计数生成函数.

2. 现有黄球两个,白球和红球各一个,试求有多少种不同的选球方式?

3. 从 n 个不同的元素中允许重复的选取 r 个元素,要求每个元素出现偶数次有多少种方式?

4. 有 6 个数字,其中 3 个 1,2 个 2,1 个 3,求能组成四位数的个数.

5. 有 n 颗人造钻石排成一行,今用红、黄、蓝、白、黑对其涂色,只要求红色有偶数颗,有

多少种涂法？

8.3 递归关系

还有一些计数问题可以归结到建立和求解递归关系．在学习数列时，有时会出现数列的后项是由前项或前几项确定的，这实际上就是递归关系，又称为递推关系．“知道他的过去，就知道他的现在；知道他的过去和现在，就知道他的将来”，体现的正是递归思想．

利用递归关系解决计数问题是很重要的方法之一，在其他数学分支中都会用到此技巧．就计算机科学来说，大多数算法的执行都表现为按某种条件重复地执行一些循环，而这些循环经常可以用递归关系来表达．因此，递归关系的建立和求解对算法分析至关重要．

本节先举例说明如何建立递归关系，再给出常用的求解递归关系的方法．部分内容讨论涉及高等数学中幂级数及其运算等有关内容．

8.3.1 递归关系的概念

我们已经知道，如果一个问题可以归结到其前面一个问题或前面一些问题，这就是递归问题，**递归**(recurrence)又称为递推．

在知道 $a_0=1$ 时，对于任意正整数 n，定义 $a_n=na_{n-1}$，这实际上是阶乘函数的递归定义或者说借助于递归给出集合$\{a_0,a_1,\cdots,a_n,\cdots\}$的定义，$a_n$ 的计算归结到其前面的一个 a_{n-1} 的计算，这时 $a_n=na_{n-1}$ 就是一个递归关系，或称为递归方程，或递归函数，其中 $a_0=1$ 称为初始条件或边界条件．为了讨论递归问题，必须给出该问题的初始条件．

给定数列 $a_0,a_1,\cdots,a_n,\cdots$，该数列中除有限项以外的任何项 a_n 与其前面一项或前面一些项的一个方程称为**递归关系**(recurrence relation)，它表示 a_n 与其前面一项或前面一些项的一种关系．为了求解该递归关系，所给出的一些条件称为**初始条件**(initial condition)．

对于数列 $a_0,a_1,\cdots,a_n,\cdots$，需要一定的技巧才能得出其递归关系，要知道 a_n 是 n 的一个解析表达式 $f(n)$有时也是比较困难的，它通常由其初始条件和递归关系来确定．我们现在感兴趣的是得出 a_n 是 n 的解析表达式，虽然一般情况下很难办到这一点．

下面是根据具体问题建立递归关系的两个例子．

【例 8-6】 (**汉诺塔**，Hanoi tower)在古印度的一座神庙里，有 3 个铜铸的基座，上面各安置一根宝石针，在一根宝石针上由大到小套了 64 个金盘．梵王命令他的僧侣，通过其余两根宝石针，把这 64 个金盘移到另外一根宝石针上(见图 8-3)．移动的规则如下：

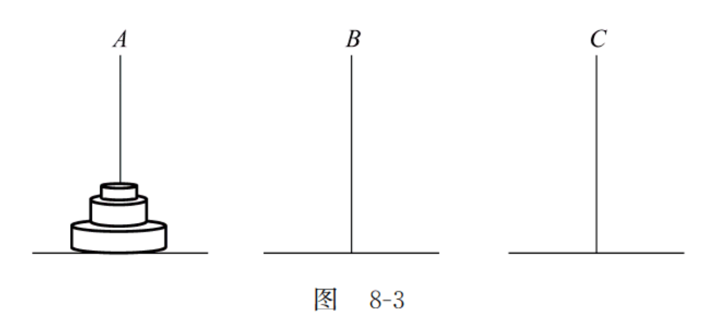


图 8-3

(1) 一次只能移动一个金盘；

(2) 金盘只能在 3 根宝石针上存放；

(3) 不允许将大金盘放在小金盘上.

假设 n 是金盘的数目(如 $n=64$),h_n 是按规则需要移动的次数,求 F_n 的初始条件以及递归关系.

解 显然,初始条件为 $h_1=1$.

当有 n 个金盘时,可以先将宝石针 A 最上面的 $n-1$ 个金盘按规则移动另外一根宝石针上,可设为 B,需要移动 h_{n-1} 次. 再将 A 上最大的金盘移动到 C,移动一次. 最后将宝石针 B 上的 $n-1$ 个金盘按规则移动到 C,又需要移动 h_{n-1} 次.

根据加法原理,有递归关系

$$h_n = 2h_{n-1}+1.$$

【例 8-7】 (**斐波那契数列**,Fibonacci sequence) 在 1202 年意大利数学家 Fibonacci 研究过兔子的繁殖问题:年初有一对小兔,雌雄各一. 小兔第一个月长大,第二个月又繁殖出一对雌雄各一的兔子. 以后,成熟的大兔每月都繁殖出一对雌雄各一的兔子,而新的每对小兔以同样规律长大、繁殖. 假定兔子都不死. 假设第 n 个月兔子有 F_n 对,求 F_n 的初始条件以及递归关系.

解 显然,初始条件为 $F_1=1,F_2=1$.

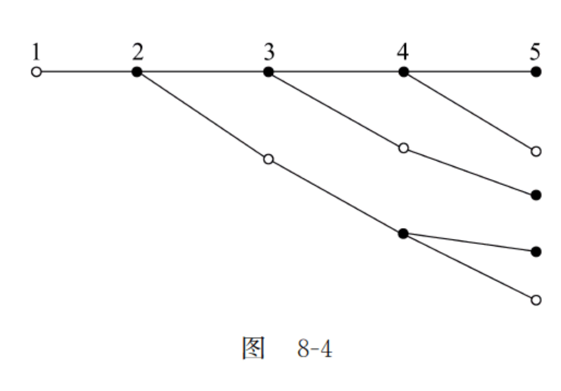


图 8-4

显然,F_n=第 n 个月大兔子的对数+第 n 个月小兔子的对数,而第 n 个月大兔子的对数=第 $n-1$ 个月兔子的对数 F_{n-1},第 n 个月小兔子的对数=第 $n-1$ 大兔子的对数=第 $n-2$ 兔子的对数 F_{n-2},见图 8-4,其中实心点表示大兔子对,空心点表示小兔子对.

根据加法原理,有递归关系

$$F_n = F_{n-1}+F_{n-2}.$$

于是,Fibonacci 数列的前 12 项为 1,1,2,3,5,8,13,21,34,55,89,144.

8.3.2 常用的递归关系求解方法

1. 递归法

递归法又称为递推法,是将对数列第 n 项 a_n 的计算转化为对其前面的一个项或一些项的计算,直到最后归结到初始条件.

【例 8-8】 在 $h_1=1$ 时,求解递归关系 $h_n=2h_{n-1}+1$.

解
$$\begin{aligned}h_n &=2h_{n-1}+1=2(2h_{n-2}+1)+1\\ &=2^2h_{n-2}+2+1=2^2(2h_{n-3}+1)+2+1\\ &=2^3h_{n-3}+2^2+2+1\\ &\ \ \vdots\\ &=2^{n-1}h_1+2^{n-2}+\cdots+2^2+2+1\\ &=2^{n-1}+2^{n-2}+\cdots+2^2+2+1=\frac{1-2^n}{1-2}=2^n-1.\end{aligned}$$

另解 由于 $h_1=1$ 且 $h_n=2h_{n-1}+1$,于是 $h_2=2h_1+1=3=2^2-1$. 进而有 $h_3=2h_2+1=7=2^3-1$. 这样一直继续下去,很容易得出 $h_n=2^n-1$.

上面的求解过程称为迭代法(iteration method),它与递归法是不同的,特别是在编写程序时数据结构设置方式是不同的.

当 $n=64$ 时,$h_{64}=2^{64}-1=18\ 446\ 744\ 073\ 709\ 551\ 615$. 若移动一次只需用 1s,约需 5845 亿年. 即使算法已经设计好了,让计算机把所有金盘的移动方式打印出来,也是很困难的. 由此可见,若一个算法的复杂度呈指数增长,那是相当可怕的.

2. 生成函数法

首先根据所给数列构造其生成函数;再利用递归关系以及已知函数的形式幂级数求出该生成函数;最后想办法得出生成函数中 x^n 或 $\frac{x^n}{n!}$ 的系数即为所求 a_n.

【例 8-9】 在初始条件 $a_1=1,a_2=1$ 下,求解递归关系 $a_n=\sum\limits_{k=1}^{n-1}a_k a_{n-k}$.

解 由数列 $a_1,a_2,\cdots,a_n,\cdots$,构造组合计数生成函数

$$G(x)=a_1x+a_2x^2+\cdots+a_nx^n+\cdots.$$

由于 $a_n=\sum\limits_{k=1}^{n-1}a_k a_{n-k}$, 于是

$$G^2(x)=a_1^2x^2+(a_1a_2+a_2a_1)x^3+\cdots+\left(\sum_{k=1}^{n-1}a_k a_{n-k}\right)x^n+\cdots$$

$$=x^2+a_3x^3+\cdots+a_nx^n+\cdots=\sum_{n=2}^{\infty}a_nx^n=G(x)-x,$$

由此可得 $G_1(x)=\frac{1+\sqrt{1-4x}}{2}$,$G_2(x)=\frac{1-\sqrt{1-4x}}{2}$. 因为 $G(0)=0$,舍去 $G_1(x)$,所以 $G(x)=\frac{1-\sqrt{1-4x}}{2}$.

利用函数 $(1+x)^m$ 的形式幂级数展开公式,有

$$\sqrt{1+x}=(1+x)^{\frac{1}{2}}=1+\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n\cdot 2^{2n-1}}C_{2n-2}^{n-1}x^n,$$

因而 $\sqrt{1-4x}=1-\sum\limits_{n=1}^{\infty}\frac{2}{n}C_{2n-2}^{n-1}x^n$,进而 $G(x)=\sum\limits_{n=1}^{\infty}\frac{1}{n}C_{2n-2}^{n-1}x^n$,故 $a_n=\frac{1}{n}C_{2n-2}^{n-1}$ (称为 Catalan 数).

【例 8-10】 在初始条件 $D_0=1$ 下,求解递归关系 $D_n=nD_{n-1}+(-1)^n(n\geqslant 1)$.

解 由数列 $D_0,D_1,\cdots,D_n,\cdots$,构造排列计数生成函数

$$E(x)=D_0+D_1x+D_2\frac{x^2}{2!}+\cdots+D_n\frac{x^n}{n!}+\cdots.$$

因为 $D_n=nD_{n-1}+(-1)^n(n\geqslant 1)$,于是

$$E(x)-1=x(E(x)-1)+\frac{x^2}{2!}-\frac{x^3}{3!}+\cdots+(-1)^n\frac{x^n}{n!}+\cdots,$$

进而,有

$$(1-x)E(x)=1-x+\frac{x^2}{2!}-\frac{x^3}{3!}+\cdots+(-1)^n\frac{x^n}{n!}+\cdots=\mathrm{e}^{-x},$$

所以,有

$$E(x)=\frac{e^{-x}}{1-x}=\left(1-x+\frac{x^2}{2!}-\frac{x^3}{3!}+\cdots+(-1)^n\frac{x^n}{n!}+\cdots\right)(1+x+\cdots+x^n+\cdots),$$

因而，$E(x)$中x^n的系数为$1-1+\frac{1}{2!}-\frac{1}{3!}+\cdots+(-1)^n\frac{1}{n!}$. 因为$D_n$为$\frac{x^n}{n!}$的系数，所以

$$D_n=\left(1-1+\frac{1}{2!}-\frac{1}{3!}+\cdots+(-1)^n\frac{1}{n!}\right)n!.$$

3. 特征方程法

对于常系数线性递归关系，可以考虑用特征方程法求解. 分两种情况进行讨论.

(1) 常系数线性齐次递归关系

设k为正整数，在初始条件$a_0,a_1,\cdots,a_{k-1}$下，递归关系

$$a_n=c_1a_{n-1}+c_2a_{n-2}+\cdots+c_ka_{n-k}\quad(n\geqslant k)\tag{1}$$

称为**k阶常系数线性齐次递归关系**(linear homogeneous recurrence relation of order k with constant coefficient)，其中$c_1,c_2,\cdots,c_k$为常数且$c_k\neq0$.

对于k阶常系数线性齐次递归关系，第n项a_n仅与其前面k项$a_{n-1},a_{n-2},\cdots,a_{n-k}$有关；系数$c_1,c_2,\cdots,c_k$为常数；关于$a_{n-1},a_{n-2},\cdots,a_{n-k}$是线性的，即不出现$a_{n-1}^2,a_{n-1}a_{n-2}$，$\sqrt{a_{n-1}}$等；同时右边不是$c_1a_{n-1}+c_2a_{n-2}+\cdots+c_ka_{n-k}+f(n)$形式，而关于$n$的函数$f(n)\neq0$.

递归关系$F_n=F_{n-1}+F_{n-2}$是二阶常系数线性齐次递归关系，而$a_n=3a_{n-1}^2+a_{n-2}$非线性，$a_n=2a_{n-1}+3$非齐次，$a_n=a_{n-1}+(n-1)a_{n-2}$非常系数.

k阶常系数线性齐次递归关系$a_n=c_1a_{n-1}+c_2a_{n-2}+\cdots+c_ka_{n-k}$的**特征方程**(characteristic equation)定义为

$$\lambda^k-c_1\lambda^{k-1}-c_2\lambda^{k-2}-\cdots-c_k=0.\tag{2}$$

就递归关系本身而言，满足它的任意一个数列称为其**特解**(special solution)，特解一般比较多. 递归关系一般解所具有的形式就是其**通解**(general solution).

由于$c_k\neq0$，其任意一个根λ均非0. 显然，$a_n=\lambda^n$是$a_n=c_1a_{n-1}+c_2a_{n-2}+\cdots+c_ka_{n-k}$的特解，即$\lambda^n=c_1\lambda^{n-1}+c_2\lambda^{n-2}+\cdots+c_k\lambda^{n-k}$当且仅当$\lambda^k=c_1\lambda^{k-1}+c_2\lambda^{k-2}+\cdots+c_k$，即$\lambda^k-c_1\lambda^{k-1}-c_2\lambda^{k-2}-\cdots-c_k=0$.

【定理 8-7】 若递归关系$a_n=c_1a_{n-1}+c_2a_{n-2}+\cdots+c_ka_{n-k}(n\geqslant k)$的特征方程$\lambda^k-c_1\lambda^{k-1}-c_2\lambda^{k-2}-\cdots-c_k=0$有$k$个不同的根$\lambda_1,\lambda_2,\cdots,\lambda_k$，则其通解为$a_n=C_1\lambda_1^n+C_2\lambda_2^n+\cdots+C_k\lambda_k^n$. 给定初始条件$a_0,a_1,\cdots,a_{k-1}$可唯一确定出其中的待定常数$C_1,C_2,\cdots,C_k$.

【例 8-11】 在初始条件$F_1=1,F_2=1$下，求解递归关系$F_n=F_{n-1}+F_{n-2}(n\geqslant3)$.

解 递归关系$F_n=F_{n-1}+F_{n-2}$的特征方程为$\lambda^2-\lambda-1=0$，其根为

$$\lambda_1=\frac{1+\sqrt5}{2},\quad\lambda_2=\frac{1-\sqrt5}{2},$$

根据定理 8-7，有$F_n=C_1\left(\frac{1+\sqrt5}{2}\right)^n+C_2\left(\frac{1-\sqrt5}{2}\right)^n$. 由于$F_1=1,F_2=1$，代入得

$$C_1=\frac{1}{\sqrt5}\left(\frac{1+\sqrt5}{2}\right),\quad C_2=-\frac{1}{\sqrt5}\left(\frac{1-\sqrt5}{2}\right),$$

所以

$$F_n=\frac{1}{\sqrt5}\left(\frac{1+\sqrt5}{2}\right)^{n+1}-\frac{1}{\sqrt5}\left(\frac{1-\sqrt5}{2}\right)^{n+1}.$$

【定理 8-8】 若递归关系 $a_n=c_1a_{n-1}+c_2a_{n-2}+\cdots+c_ka_{n-k}(n\geqslant k)$的特征方程 $\lambda^k-c_1\lambda^{k-1}-c_2\lambda^{k-2}-\cdots-c_k=0$ 有 t 个不同的根 $\lambda_1,\lambda_2,\cdots,\lambda_t$,其重数分别为 $r_1,r_2,\cdots,r_t(r_1+r_2+\cdots+r_t=k)$,则其解为 $a_n=a_1(n)+a_2(n)+\cdots+a_t(n)$,其中 $a_i(n)=(C_{1i}+C_{2i}n+\cdots+C_{r_i i}n^{r_i-1})\lambda_i^n$,$i=1,2,\cdots,t$.给定初始条件 $a_0,a_1,\cdots,a_{k-1}$可唯一确定出其中的所有待定常数.

实际上,定理 8-8 推广了定理 8-7.

【例 8-12】 在初始条件 $a_0=1,a_1=2,a_2=7$ 下,求解递归关系

$$a_n=5a_{n-1}-7a_{n-2}+3a_{n-3}\quad(n\geqslant 3).$$

解 递归关系 $a_n=5a_{n-1}-7a_{n-2}+3a_{n-3}$的特征方程为 $\lambda^3-5\lambda^2+7\lambda-3=0$,其根为 $\lambda_1=1$(二重根),$\lambda_2=3$,于是

$$a_n=(C_1+C_2n)1^n+C_33^n=C_1+C_2n+C_33^n.$$

将初始条件 $a_0=1,a_1=2,a_2=7$ 代入,得

$$a_0=C_1+0C_2+C_33^0=C_1+C_3=1,$$
$$a_1=C_1+1C_2+C_33^1=C_1+C_2+3C_3=2,$$
$$a_2=C_1+2C_2+C_33^2=C_1+2C_2+9C_3=7,$$

于是 $C_1=0,C_2=-1,C_3=1$,进而

$$a_n=3^n-n.$$

(2) 某些常系数线性非齐次递归关系

设 k 为正整数,在初始条件 $a_0,a_1,\cdots,a_{k-1}$下,递归关系

$$a_n=c_1a_{n-1}+c_2a_{n-2}+\cdots+c_ka_{n-k}+f(n)\quad(n\geqslant k)\tag{3}$$

称为 **k 阶常系数线性非齐次递归关系**(linear non-homogeneous recurrence relation of order k with constant coefficient),其中 $c_1,c_2,\cdots,c_k$ 为常数,$c_k\neq 0$,非齐次项 $f(n)$是关于 n 的函数且 $f(n)\neq 0$.

对于一般的非齐次项 $f(n)$没有统一的求解方法.一般情况下有下述定理,但人们仍希望能直接求解或想办法转化成常系数线性齐次递归关系求解.

【定理 8-9】 若 k 阶常系数线性非齐次递归关系 $a_n=c_1a_{n-1}+c_2a_{n-2}+\cdots+c_ka_{n-k}+f(n)(n\geqslant k)$有特解 b_n,且对应的 k 阶常系数线性齐次递归关系 $a_n=c_1a_{n-1}+c_2a_{n-2}+\cdots+c_ka_{n-k}$的通解为 B_n,则 $a_n=c_1a_{n-1}+c_2a_{n-2}+\cdots+c_ka_{n-k}+f(n)$的通解为 $a_n=B_n+b_n$.给定初始条件 $a_0,a_1,\cdots,a_{k-1}$可唯一确定出其中的所有待定常数.

【例 8-13】 在初始条件 $a_1=2$ 下,求解递归关系

$$a_n=a_{n-1}+3^n\quad(n\geqslant 2).$$

解 因为 $a_n=a_{n-1}+3^n$,所以 $a_{n-1}=a_{n-2}+3^{n-1}$,$a_{n-2}=a_{n-3}+3^{n-2}$,$\cdots$, $a_2=a_1+3^2$,将这些等式左右两边分别相加并整理得

$$a_n=a_1+3^2+3^3+\cdots+3^n,$$

于是

$$a_n=2+\frac{9}{2}(3^{n-1}-1).$$

【例 8-14】 求 $a_n=1^2+2^2+\cdots+(n-1)^2+n^2$.

解 根据题意,有 $a_{n-1}=1^2+2^2+\cdots+(n-1)^2$,于是 $a_n=a_{n-1}+n^2$,这是一个一阶常系

数线性非齐次递归关系．由于 $a_n=0^2+1^2+2^2+\cdots+(n-1)^2+n^2$，因此，$a_0=0$，$a_1=1$，$a_2=5$，$a_3=14$．

由于 $a_n=a_{n-1}+n^2$，进而 $a_{n-1}=a_{n-2}+(n-1)^2$，相减并整理得

$$a_n = 2a_{n-1} - a_{n-2} + 2n - 1.$$

由此可得 $a_{n-1}=2a_{n-2}-a_{n-3}+2(n-1)-1$，再相减并整理得

$$a_n = 3a_{n-1} - 3a_{n-2} - a_{n-3} + 2.$$

因而 $a_{n-1}=3a_{n-2}-3a_{n-3}-a_{n-4}+2$，再相减并整理得

$$a_n = 4a_{n-1} - 6a_{n-2} + 4a_{n-3} + a_{n-4},$$

这是一个四阶常系数线性齐次递归关系，其特征方程为 $\lambda^4-4\lambda^3+6\lambda^2-4\lambda+1=0$，其根为 $\lambda=1$（四重根），于是

$$a_n = (C_1 + C_2 n + C_3 n^2 + C_4 n^3)1^n = C_1 + C_2 n + C_3 n^2 + C_4 n^3.$$

将初始条件 $a_0=0$，$a_1=1$，$a_2=5$，$a_3=14$ 代入，得

$$\begin{cases} C_1 = 0 \\ C_2 + C_3 + C_4 = 1 \\ 2C_2 + 4C_3 + 8C_4 = 5 \\ 3C_2 + 9C_3 + 27C_4 = 14 \end{cases}$$

于是 $C_1=0$，$C_2=\dfrac{1}{6}$，$C_3=\dfrac{1}{2}$，$C_4=\dfrac{1}{3}$，进而

$$a_n = \frac{1}{6}n + \frac{1}{2}n^2 + \frac{1}{3}n^3 = \frac{1}{6}n(n+1)(2n+1).$$

4．其他方法

【例 8-15】 在初始条件 $f(1)=1$ 下，求解递归关系 $f(n)=2f\left(\dfrac{n}{2}\right)+\dfrac{n}{2}-1$，其中 $n=2^k$，k 为正整数．

解 令 $g(k)=f(2^k)=f(n)$，于是原递归关系变为

$$\begin{cases} g(k) = 2g(k-1) + 2^{k-1} - 1 \\ g(0) = 1 \end{cases}.$$

利用递归法，有

$$\begin{aligned} g(k) &= 2[2g(k-2) + 2^{k-2} - 1] + 2^{k-1} - 1 \\ &= 2^2 g(k-2) + 2 \times 2^{k-1} - 2 - 1 \\ &= 2^3 g(k-3) + 3 \times 2^{k-1} - 2^2 - 2 - 1 \\ &\vdots \\ &= 2^k g(0) + k2^{k-1} - \sum_{i=0}^{k-1} 2^i \\ &= 2^k + k2^{k-1} - (2^k - 1) \\ &= k2^{k-1} + 1 \\ &= \frac{1}{2}n\ln n + 1, \end{aligned}$$

因此,有 $f(n)=\frac{1}{2}n\ln n+1$,其中 $n=2^k$,k 为正整数.

习　题　8.3

1. 某人举步上楼梯,每步跨 1 个台阶或 2 个台阶,设上 n 个台阶的不同方式数为 a_n. 求出关于 a_n 的初始条件以及递归关系.

2. 设有 n 个数 $A_1, A_1, \cdots, A_n$ 连乘积 $A_1A_1\cdots A_n$,其不同的结合方式用 a_n 表示,求出关于 a_n 的初始条件以及递归关系.

3. 有 n 根火柴,甲、乙二人轮流来取,每次仅能取 1 根或 2 根. 若甲先取,最后还由甲取光的方案数为 a_n. 求出关于 a_n 的初始条件以及递归关系.

4. 用递归法求解递归关系 $a_0=0, a_n=na_{n-1}+n!\ (n\geqslant 1)$.

5. 用递归法求解递归关系 $a_0=2, a_n^2=2a_{n-1}^2+1(n\geqslant 1)$.

6. 利用生成函数求解递归关系 $\begin{cases} a_n=a_{n-1}+2(n-1) \\ a_1=2 \end{cases}$.

7. 在初始条件 $a_0=1, a_1=1$ 下,求解递归关系

$$(n-1)a_n=(n-2)a_{n-1}+2a_{n-2}.$$

8. 在初始条件 $a_0=0, a_1=2, a_2=10$ 下,求解递归关系 $a_n=6a_{n-1}-11a_{n-2}+6a_{n-3}$ $(n\geqslant 3)$.

9. 在初始条件 $a_0=1, a_1=0, a_2=1, a_3=2$ 下,求解递归关系

$$a_n=-a_{n-1}+3a_{n-2}+5a_{n-3}+2a_{n-4}\quad (n\geqslant 4).$$

10. 在初始条件 $a_0=1, a_1=2$ 下,求解递归关系

$$a_n=7a_{n-1}-10a_{n-2}+4n^2\quad (n\geqslant 2).$$

11. 使用定理 8-9,在初始条件 $a_0=1, a_1=2$ 下,求解递归关系

$$a_n=7a_{n-1}-12a_{n-2}+n2^n\quad (n\geqslant 2).$$

12. 在初始条件 $f(1)=c$ 下,求解递归关系 $f(n)=2f\left(\frac{n}{2}\right)+bn$,其中 b,c 为常数且 $n=2^k$,k 为正整数.

本 章 小 结

1. 计数原理、排列组合与二项式定理

理解加法原理和乘法原理,要清楚何时相加、何时相乘. 记住下列几种情形的计数公式:

n 个元素的 r-排列个数

$$P_n^r=n(n-1)\cdots(n-r+1)=\frac{n!}{(n-r)!}$$

n 个元素的 r-圆排列个数

$$\odot P_n^r=\frac{P_n^r}{r}.$$

n 个元素的 r-可重排列个数

$$U_n^r = n^r.$$

设 $A=\{n_1 \cdot A_1, n_2 \cdot A_2, \cdots, n_k \cdot A_k\}$, $n_1+n_2+\cdots+n_k=n$，这 n 个元素的全排列个数为

$$\frac{n!}{n_1!n_2!\cdots n_k!}.$$

n 个元素的 r-组合个数

$$C_n^r = \frac{P_n^r}{r!} = \frac{n(n-1)\cdots(n-r+1)}{r!} = \frac{n!}{(n-r)!r!}$$

n 个元素的 r-可重组合个数

$$F_n^r = C_{n+r-1}^r.$$

2. 生成函数

(1) 对于数列 $a_0, a_1, \cdots, a_r, \cdots$,其组合计数生成函数

$$G(x) = a_0 + a_1x + \cdots + a_rx^r + \cdots = \sum_{r=0}^{\infty} a_rx^r.$$

掌握利用组合计数生成函数解决一般的组合计数问题的思想.

(2) 对于数列 $a_0, a_1, \cdots, a_r, \cdots$,其排列计数生成函数为

$$E(x) = a_0 + a_1x + a_2\frac{x^2}{2!} + \cdots + a_r\frac{x^r}{r!} + \cdots = \sum_{r=0}^{\infty} a_r\frac{x^r}{r!},$$

排列个数 a_r 是$\frac{x^r}{r!}$的系数.

定理 设 $A_1, A_2, \cdots, A_k$ 是 k 个不同元素,现有 n_i 个 A_i 元素($i=1,2,\cdots,k$, $n_1+n_2+\cdots+n_k=n$),在这 n 个元素中任取 r 个元素的排列个数为 a_r,则其排列计数生成函数为

$$\begin{aligned}&a_0 + a_1x + a_2\frac{x^2}{2!} + \cdots + a_r\frac{x^r}{r!} + \cdots \\ =&\left(1+x+\frac{x^2}{2!}+\cdots+\frac{x^{n_1}}{n_1!}\right)\left(1+x+\frac{x^2}{2!}+\cdots+\frac{x^{n_2}}{n_2!}\right)\cdots\left(1+x+\frac{x^2}{2!}+\cdots+\frac{x^{n_k}}{n_k!}\right).\end{aligned}$$

掌握利用排列计数生成函数解决一般的排列计数问题的思想.

3. 递归关系

熟悉递归关系的建立.

掌握常用的求解递归关系的方法:递归法、生成函数法、特征方程法和其他方法.

k 阶常系数线性齐次递归关系 $a_n=c_1a_{n-1}+c_2a_{n-2}+\cdots+c_ka_{n-k}$ 的特征方程为

$$\lambda^k - c_1\lambda^{k-1} - c_2\lambda^{k-2} - \cdots - c_k = 0.$$

主要定理 若递归关系 $a_n=c_1a_{n-1}+c_2a_{n-2}+\cdots+c_ka_{n-k}$ ($n\geqslant k$)的特征方程 $\lambda^k-c_1\lambda^{k-1}-c_2\lambda^{k-2}-\cdots-c_k=0$ 有 t 个不同的根 $\lambda_1, \lambda_2, \cdots, \lambda_t$,其重数分别为 $r_1, r_2, \cdots, r_t$ ($r_1+r_2+\cdots+r_t=k$),则其解为 $a_n=a_1(n)+a_2(n)+\cdots+a_t(n)$,其中 $a_i(n)=(C_{1i}+C_{2i}n+\cdots+C_{r_ii}n^{r_i-1})\lambda_i^n$, $i=1,2,\cdots,t$. 给定初始条件 $a_0, a_1, \cdots, a_{k-1}$ 可唯一确定出其中的所有待定常数.

附录 A　符号索引

符　号	含　义	符　号	含　义
U	全集	xRy	x 与 y 有关系 R
$x\in A$	x 属于 A	$\equiv_k$	模 k 同余关系
$x\notin A$	x 不属于 A	$\mathrm{dom}R$	关系 R 的定义域
$\|A\|$	集合 A 的基数；有限集合的元素个数	$\mathrm{ran}R$	关系 R 的值域
$\varnothing$	在集合运算中表示空集	G_R	关系图
$A\subseteq B$	A 是 B 的子集	$\boldsymbol{M}_R$	关系矩阵
$A=B$	集合相等	$R\cup S$	关系 R 与 S 的并
$A\subset B$	A 是 B 的真子集	$R\cap S$	关系 R 与 S 的交
$P(X)$，2^X	X 的幂集	$R-S$	关系 R 与 S 的差
$(x_1,x_2,\cdots,x_n)$	元组	$\overline{R}$	关系 R 的补
$A_1\times A_2\times\cdots\times A_n$	笛卡儿积	$R\oplus S$	关系 R 与 S 的对称差（环和）
$f:A\to B$	映射，函数	R^{-1}	逆关系
$\mathrm{dom}f$	定义域	$R\circ S$	复合关系
$\mathrm{ran}f$	值域	R^n	关系的幂运算
B^A	A 到 B 的所有映射组成的集合	$R\|_B$	R 在 B 上的限制
$f(X)$	X 在映射 f 下的像	$r(R)$	自反闭包
$f^{-1}(Y)$	Y 在映射 f 下的原像	$s(R)$	对称闭包
f^{-1}	逆映射，逆函数，反函数	$t(R)$	传递闭包
$g\circ f$	映射 f 和 g 的复合	$[x]_R$	等价类
I_A	A 上的恒等映射，A 上的恒等关系	A/R	商集
$A\cup B$	集合 A 与 B 的并	$\mathrm{lub}(S)$或$\sup(S)$	上确界
$A\cap B$	集合 A 与 B 的交	$\mathrm{glb}(S)$或$\inf(S)$	下确界
$\overline{A}$	集合 A 的补集	1，T	真
$A-B$	集合 A 与 B 的差	0，F	假
$A\oplus B$	A 与 B 的对称差，A 与 B 的环和	$\neg p$	非 p

续表

符　号	含　　义	符　号	含　　义
$A \sim B$	A 和 B 对等	$p \wedge q$	合取
$\lvert A \rvert \leqslant \lvert B \rvert$	A 的基数小于等于 B 的基数	$p \vee q$	析取
$\lvert A \rvert < \lvert B \rvert$	A 的基数小于 B 的基数	$p \oplus q$	异或
R	关系	$p \rightarrow q$	蕴涵
$\varnothing$	在关系运算中表示空关系	$p \leftrightarrow q$	等价
$A \times B$	A 到 B 的全关系	$p \uparrow q$	与非
$p \downarrow q$	或非	$\delta^{-}(G)$	最小入度
$p \stackrel{n}{\rightarrow} q$	条件否定	$G[W]$	由 W 导出的子图
$A = B$	逻辑等值	$G - W$	$G[V-W]$
A^{*}	对偶式	$G[F]$	由 F 导出的子图
$H_1, H_2, \cdots, H_n \Rightarrow C$	有效推理形式	$G - F$	去掉 F 中的所有边得到的生成子图
US	全称量词消去规则	$G + U$	增加新边 U
UG	全称量词产生规则	$G_1 \cup G_2$	图的并
ES	存在量词消去规则	$G_1 \cap G_2$	图的交
EG	存在量词产生规则	$G_1 - G_2$	图的差
$A \cong B$	同构	$G_1 \oplus G_2$	图的对称差(环和)
S_n	n 次对称群	$G_1 \cong G_2$	图同构
$H \leqslant G$	子群	$d(u,v)$	距离
aH	左陪集	$\mathrm{diam}(G)$	直径
Ha	右陪集	$w(G)$	连通分支数
$N \lhd G$	正规子群	$\kappa(G)$	点连通度
G/N	商群	$\lambda(G)$	边连通度
$\mathrm{Ker}\varphi$	核	$\boldsymbol{A}(G)$	邻接矩阵
$\mathrm{GF}(q)$	有限域	$\boldsymbol{P}(G)$	可达矩阵
$(L, \leqslant)$	偏序格	$\boldsymbol{M}(G)$	关联矩阵
$x + y$	求上确界	G^{*}	对偶图
$x \cdot y$	求下确界	$\chi(G)$	节点着色数
$(L, +, \cdot)$	代数格	$K_{m,n}$	完全二部图
$(B, \leqslant)$	布尔格	$m \mid n$	m 整除 n
$(B, +, \cdot, ^{-},)0, 1$	布尔代数	P_n^r 或 $P(n, r)$	n 个元素的 r-排列

续表

符　号	含　　义	符　号	含　　义
$G=(V,E)$	图	C_n^r 或 $\binom{n}{r}$ 或 $C(n, r)$	n 个元素的 r-组合
uv	无向边	D_n	n 的所有正因数组成的集合
(u,v)，$<u,v>$	有向边	$\lceil x \rceil$	天花板函数
$\varnothing$	在图论中表示空图	$\lfloor x \rfloor$	地板函数，取整函数
K_n	完全无向图	$x(\bmod m)$	模 m 运算
$\bar{G}$	补图	$\gcd(m,n)$	最大公因数
$\deg(v)$	度数	$\operatorname{lcm}(m,n)$	最小公倍数
$\operatorname{od}(v)$	出度	$\varphi(n)$	欧拉函数
$\operatorname{id}(v)$	入度	$Z_m=\{0, 1, 2, \cdots, m-1\}$	$0, 1, 2, \cdots, m-1$ 组成的集合
$\Delta(G)$	最大度	$\equiv_m$	模 m 同余关系
$\delta(G)$	最小度	$\odot P_n^r$ 或 $\odot P(n, r)$	n 个元素的 r-圆排列
$\Delta^+(G)$	最大出度	U_n^r 或 $U(n, r)$	n 个元素的 r-可重排列
$\delta^+(G)$	最小出度	F_n^r 或 $F(n, r)$	n 个元素的 r-可重组合
$\Delta^-(G)$	最大入度		

附录 B　中英文名词索引

中文	英文
集合	set
元素	element
全集	universal set
因数	divisor
整除	divide
素数	prime
合数	composite number
递归，递推	recurrence
计数	counting
加法原理	addition principle
乘法原理	multiplication principle
排列	permutation
组合	combination
模糊集合	fuzzy set
空集	empty set
子集	subset
真子集	proper subset
n 元组	ordered n-tuple
笛卡儿积	Cartesian product
映射	mapping
函数	function
变换	transformation
天花板函数	ceiling function
地板函数	floor function
定义域	domain
值域	range
像	image
原像	inverse image
单射	injection, one-to-one
满射	surjection, onto
双射	bijection, one-to-one correspondence
置换	permutation
逆函数，逆映射，反函数	invertible function
复合函数	composition function
恒等映射	identity function
运算	operation
封闭运算，代数运算	closed operation, algebraic operation
商	quotient
余数	remainder
密文	ciphertext
密钥	key
散列函数或哈希函数	Hash function
公因数	common divisor
最大公因数	greatest common divisor
公倍数	common multiple
最小公倍数	least common multiple
互素	coprime
欧拉函数	Euler function
对合性	involutive property
幂等元	idempotent element
幂等性	idempotent property
交换性	commutative property
结合性	Associative property
单位元素或幺元素	identity element
零元素	zero element
逆元素	invertible element
消去性	cancellation property
分配性	distributive property
吸收性	absorptive property
德摩根律	De Morgan law
并	union
交	intersection
补	complement
差	subtraction
对称差，环和	symmetric difference, ring sum
第一数学归纳法	first mathematical induction
第二数学归纳法	second mathematical induction

容斥原理	inclusion-exclusion principle
划分	partition
块	block
覆盖	covering
粗糙集	rough set
对等	equivalent to
无限集合	infinite set
有限集合	finite set
基数	cardinality, cardinal number
可列集合	countable set
不可列集合	uncountable set
n 元关系	n-ary relation
关系的定义域	domain of relation
关系的值域	range of relation
关系图	graph of relation
关系矩阵	matrix of relation
逆关系	ionverse
复合关系	composition
关系的幂运算	power of relation
关系的限制	restriction of relation
自反性	reflexive
反自反性	irreflexive
对称性	symmetric
反对称性	antisymmetric
传递性	transitive
自反闭包	reflexive closure
对称闭包	symmetric closure
传递闭包	transitive closure
等价关系	equivalent relation
等价类	equivalent class
商集	quotient set
相容关系	compatible relation
相容类	compatible class
极大相容类	maximal compatible class
偏序	partial order
偏序集	poset
线性序,全序	linear order,total order
汉斯图	Hasse digram
链	chain
最大元	greatest element
最小元	least element
极大元	maximal element
极小元	minimal element
上界	upper bound
下界	lower bound
上确界	least upper bound
下确界	greatest lower bound
命题	proposition, statement
真值	truth
原子命题	atom
复合命题	compound statement
逻辑常量	logical constant
命题变元,逻辑变量	proposition variable, logical variable
逻辑联结词	logical connectives
否定	negation, not
合取	conjunction, and
析取	disjunction, or
异或	exclusive or, XOR
蕴涵	implication, if…then
前件	antecedent
后件	consequent
等价	equivalence,if and only if
命题公式	proposition formula
真值指派,解释	assignment,interpretation
真值表	truth table
永真式或重言式	tautology
永假式或矛盾式	contradiction
可满足式	satisfactable formula
逻辑等值	logically equal
对偶式	dual formula
析取范式	disjunctive normal form
合取范式	conjunctive normal form
最小项	minimal term
主析取范式	major disjunctive form
最大项	maximal term
主合取范式	major conjunctive form
功能完备联结词集	complete group of connectives
推理形式有效	valid argument form
前提	antecedent, premise, hypothesis
结论	conclusion
个体	individual

个体域	domain of individuals
谓词	predicate
存在量词	existential quantifier
作用域或辖域	scope,domain of variables
约束变元	bound variable
自由变元	free variable
函词	function
谓词公式	predicate formula
永真式或有效式	valid
前束范式	prenex normal form
全称量词消去规则	universal quantifier specification
全称量词产生规则	universal quantifier generalization
存在量词消去规则	existential quantifier specification
存在量词产生规则	existential quantifier generalization
代数结构	algebra structure
半群	semigroup
独异点	monoid
子代数	subalgebra
同态	homomorphism
同构	isomorphism
群	group
有限群	finite group
无限群	infinite group
对称群	symmetric group
置换群	permutation group
交换群,阿贝尔群	commutative group,Abelian group
元素的阶	element order
循环群	cyclic group
生成元	generator
子群	subgroup
左陪集	left coset
右陪集	right coset
正规子群	normal subgroup
商群	quotient group
同余关系	congruence relation
核	kernel
环	ring
整环	integral domain
子环	subring
理想	ideal
域	field
域的特征	characteristic
有限域,Galois 域	finite field
偏序格	lattice
子格	sublattice
分配格	distributive lattice
有界格	bounded lattice
有补格	lattice complemented
布尔代数，布尔格	Boolean algebra
有限布尔代数	finite Boolean algebra
布尔表达式	Boolean expression
布尔函数	Boolean function
图	graph
无向边	edge
有向边,弧	edge，arc
无向图	graph，undirected graph
有向图	digraph，directed graph
空图	empty graph
平凡图	trivial graph
零图	discrete graph
邻接	adjacent
关联	incident
自环	loop
多重边	multiple edges
简单图	simple graph
完全无向图	complete graph
彼得森图	Petersen graph
补图	complementary graph
度数	degree
出度	out-degree
入度	in-degree
孤立点	isolated vertex
悬挂点	pendant vertex
k-正则图	k-regular graph
子图	subgraph
生成子图	spanning subgraph
导出子图	induced subgraph
路	walk，way
路的长度	length of walk,hop number
路径	path
轨迹	trail

距离	distance
直径	diameter
回路	circuit
圈或环	cycle
简单回路	closed trail
可达	accessible
连通图	connected graph
连通分支	connected component
点割集	cut-set of vertices
割点	cut point
点连通度	vertex-connectivity
边割集	cut-set of edges
割边或桥	bridge
边连通度	edge-connectivity
强连通图	strongly connected digraph
强连通分支	strongly connected component
单向连通图	unilateral connected digraph
单向连通分支	unilateral connected component
弱连通图	weakly connected digraph
弱连通分支	weakly connected component
邻接矩阵	adjacency matrix
可达矩阵	accessible matrix
关联矩阵	incidence matrix
赋权图	weighted graph
欧拉轨迹	Eulerian trail
欧拉回路	Eulerian circuit
欧拉图	Eulerian graph
中国邮递员问题	Chinese postman problem
哈密尔顿路径	Hamiltonian path
哈密尔顿回路	Hamiltonian cycle
哈密尔顿图	Hamiltonian graph
货郎担问题或旅行商问题	traveling salesman problem
无向树	tree
树枝	branch
叶	leaf
森林	forest
生成树	spanning tree
弦	chord
基本回路	fundamental cycle
基本回路系统	fundamental cycle set
基本割集	fundamental cut set
基本割集系统	fundamental cut set system
最小生成树	minimal spanning tree
有向树	directed tree
父节点	parent
子节点	child
根树	rooted tree
树根	root
祖先	ancestor
后代	offspring, descendants
层	level
高度,深度	height,depth
子根树,子树	rooted subtree,subtree
m-叉树	m-ary tree
赫夫曼树	Huffman tree
有序树	ordered tree
有序森林	ordered forest
定位二叉树	positional binary tree
前缀码	prefix code
可平面图	planar graph
平面图	plane graph
极大平面图	maximal planar graph
极小非平面图	minimal nonplanar graph
面	face
边界	boundary
同胚	homeomorphism
对偶图	dual graph
面着色	face coloring
面着色数	region chromatic number
节点着色	vertex coloring
节点着色数	chromatic number
边着色	edge coloring
边(着)色数	edge chromatic number
Ramsey 问题	Ramsey problem
二部图	bipartite graph
完全二部图	complete bipartite graph
匹配,边独立集	matching,independent set of edges
最大匹配	maximum matching
完美匹配	perfect matching
完备匹配	complete matching
圆排列	circular permutation
可重排列	permutation with repetition
可重组合	combination with repetition
生成函数,母函数	generating function
组合计数生成函数	ordinary generating function

排列计数生成函数	exponential generating function	特征方程	characteristic equation
递归关系	recurrence relation	特解	special solution
初始条件	initial condition	通解	general solution
k 阶常系数线性齐次递归关系	linear homogeneous recurrence relation of order k with constant coefficient	k 阶常系数线性非齐次递归关系	linear non homogeneous recurrence relation of order k with constant coefficient

附录 C　习题答案及提示

习题 1.1

1. (1) $\{x \mid x\in\mathbf{R}, x^2-5x+6=0\}=\{2,3\}$.

   (2) $\{2x \mid x\in\mathbf{N}\}=\{0,2,4,6,\cdots,2x,\cdots\}$.

2. 35 的所有因数集合为$\{-35, -7, -5, -1, 1, 5, 7, 35\}$,$D_{35}=\{1, 5, 7, 35\}$.

3. $\varnothing$是空集,它里面没有元素;$\{\varnothing\}$是由空集$\varnothing$组成的集合,它里面有一个元素$\varnothing$;$\{\{\varnothing\}\}$里面有一个元素为$\{\varnothing\}$,但$\{\varnothing\}$与$\varnothing$是不同的.

4. (1) 成立.(2) 不成立.(3)成立.(4) 成立.

5. $A=\{a,b\}, B=\{a,b,\{a,b\},c\}$.

6. (1) 不成立.(2) 不成立.(3) 不成立.(4) 不成立.

7. (1) $\{\varnothing,\{\varnothing\}\}$.(2) $\{\varnothing, \{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},\{a,b,c\}\}$.
(3) $\{\varnothing, \{\{a,b,c\}\}\}$.

10.

$$A\times A=\{(a,a),(a,b),(b,a),(b,b)\}.$$
$$A\times B=\{(a,1),(a,2),(a,3),(b,1),(b,2),(b,3)\}.$$
$$B\times A=\{(1,a),(1,b),(2,a),(2,b),(3,a),(3,b)\}.$$
$$A\times B\times A=\{(a,1,a),(a,1,b),(a,2,a),(a,2,b),(a,3,a),(a,3,b),$$
$$\{(b,1,a),(b,1,b),(b,2,a),(b,2,b),(b,3,a),(b,3,b)\}.$$
$$(A\times B)\times A=\{((a,1),a),((a,1),b),((a,2),a),((a,2),b),((a,3),a),$$
$$((a,3),b),((b,1),a),((b,1),b),((b,2),a),((b,2),b),$$
$$((b,3),a),((b,3),b)\}.$$

11. 若 $A=\varnothing$,不能得出 $B=C$;若 $A\neq\varnothing$,则 $B=C$.

习题 1.2

1. $\lceil 1.5\rceil=2, \lceil -1\rfloor=-1, \lceil -1.5\rceil=-1, \lfloor 1.5\rfloor=1, \lfloor -1\rfloor=-1, \lfloor -1.5\rfloor=-2$.

2. (1) f 是单射,f 不是满射,f 不是双射.(2) f 不是单射,f 不是满射,f 不是双射.(3) f 是单射,f 是满射,f 是双射.(4) f 不是单射,f 不是满射,f 不是双射.(5) f 是单射,f 不是满射,f 不是双射.

3. 举例 $f:\mathbf{N}\to\mathbf{N}, f(x)=2x$.

5. 令 $A=\{a,b,c\}, f(a)=f(b)=f(c)=a$,即对于任意 $x\in A, f(x)=a$,显然 $f:A\to A$ 且 $f\neq I_A$. 而对于任意 $x\in A$,有$(f\circ f)(x)=f(f(x))=f(a)=a$,因此 $f\circ f=f$. 若 f 的逆映射存在,满足条件的 f 不存在.

7. 例如 $A=\{a,b\}, B=\{1,2,3\}, C=\{\alpha,\beta,\gamma,\delta\}$,令 $f(a)=1, f(b)=2, g(1)=\alpha, g(2)=\beta, g(3)=\beta$,则显然有$(f\circ g)(a)=g(f(a))=g(1)=\alpha$, $(f\circ g)(b)=g(f(b))=g(2)=\beta$,于是 $g\circ f$ 是 A 到 C 的单射,但 g 显然不是单射.

11. 6,0,0. 若 $m<n$,不存在满射;若 $m\geqslant n$,A 到 B 的满射共有 $S(m,n)\cdot n!$ 个. 若

$m>n$，不存在单射；若 $m\leqslant n$，A 到 B 的单射共有 $C_n^m \cdot m!$ 个. 若 $m\neq n$，不存在双射；若 $m=n$，A 到 B 的双射共有 $m!$ 个.

13. $f^{-1}=g\circ h, g^{-1}=h\circ f, h^{-1}=f\circ g$.

14. $A(2,3)=9, A(3,2)=29$.

习题 1.3

1. 减法运算"－"不是，其余均是.

2. $3^1+3^2=12\notin A$.

3. 3^9.

4. $(555)_8$.

5. $16 \pmod 3)=1, -16 \pmod 3)=2, 0 \pmod 3)=0$.

6. $\gcd(36, 48)=2^2\times 3=12, \operatorname{lcm}(36, 48)=2^4\times 3^2=144$.

7. $\gcd(14, 158)=2, 2=14\times 4+158\times(-3)$.

8. 表 1-6：不满足幂等性、满足交换性、1 是单位元素、1 的逆元为 1，2 和 3 都没有逆元.

表 1-7：满足幂等性、不满足交换性、1 是单位元素、1 的逆元为 1，2 和 3 都没有逆元.

15. $p_1(1)=1, p_1(2)=2, p_1(3)=3; p_2(1)=2, p_2(2)=1, p_2(3)=3;$

$p_3(1)=3, p_3(2)=2, p_3(3)=1; p_4(1)=1, p_4(2)=3, p_4(3)=2;$

$p_5(1)=2, p_5(2)=3, p_5(3)=1; p_6(1)=3, p_6(2)=1, p_6(3)=2.$

列出 G 关于映射的复合"$\circ$"的运算表如表 C-1 所示.

表 C-1

$\circ$	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_1	p_5	p_6	p_3	p_4
p_3	p_3	p_6	p_1	p_5	p_4	p_2
p_4	p_4	p_5	p_6	p_1	p_2	p_3
p_5	p_5	p_4	p_2	p_3	p_6	p_1
p_6	p_6	p_3	p_4	p_2	p_1	p_5

(2)由运算表可知，对于任意 $p_i\in G$，有 $p_i\circ(1)(2)(3)=(1)(2)(3)\circ p_i=p_i$，所以 (1)、(2)、(3)是 G 关于复合映射"$\circ$"的单位元素.

由运算表可知，$p_1^{-1}=p_1, p_2^{-1}=p_2, p_3^{-1}=p_3, p_4^{-1}=p_4, p_5^{-1}=p_6, p_6^{-1}=p_5$.

习题 1.4

1. (1) $A\cup B=\{a,b,c,d,e,f,g\}$.

(2) $B\cap C=\{f\}$.

(3) $A-D=\{a,b,c,g\}$.

(4) $(A\cap B)-C=\{g\}-C=\{g\}-\{a,c,f\}=\{g\}$.

(5) $\overline{D}=\{a,b,c,d,e,g\}$.

(6) $B\oplus C=(B\cup C)-(B\cap C)=\{a,c,d,e,f,g\}-\{f\}=\{a,c,d,e,g\}$.

(7) $A\cap(B\cup C)=\{a,b,c,g\}\cap\{a,c,d,e,f,g\}=\{a,c,g\}$.

(8) $(A\cup D)-\overline{C}=\{a,b,c,g,f,h\}-\{b,d,e,g,h\}=\{a,c,f\}$.

(9) $\overline{A\cup C}=\overline{\{a,b,c,f,g\}}=\{d,e,h\}$.

(10) $A\cup B\cup C=\{a,b,c,d,e,f,g\}$.

5. 例如取 $A=\{a,b,c\}$, $B=\{1,2\}$,令 $f:A\to B$, $f(a)=f(b)=2$, $f(c)=1$. 再取 $X=\{a,c\}$, $Y=\{b,c\}$,这时 $f(X)=\{1,2\}$, $f(Y)=\{1,2\}$,因此 $f(X)\cap f(Y)=\{1,2\}$. 由于 $f(X\cap Y)=f(\{c\})=\{1\}$,所以有 $f(X\cap Y)\neq f(X)\cap f(Y)$.

7. (1) 不成立. (2) 不成立. (3) 成立.

8. (2) 因为 $A\subseteq A\cup B$,于是 $P(A)\subseteq P(A\cup B)$. 同样, $P(B)\subseteq P(A\cup B)$,所以 $P(A)\cup P(B)\subseteq P(A\cup B)$.

例如 $A=\{a,b\}$, $B=\{b,c\}$,于是 $P(A)=\{\varnothing,\{a\},\{b\},\{a,b\}\}$ 且 $P(B)=\{\varnothing,\{b\},\{c\},\{b,c\}\}$,因此

$$P(A)\cup P(B)=\{\varnothing,\{a\},\{b\},\{c\},\{a,b\},\{b,c\}\},$$

这时 $|P(A)\cup P(B)|=6$. 而 $A\cup B=\{a,b,c\}$,所以 $|P(A\cup B)|=2^3=8$. 显然有 $P(A)\cup P(B)\neq P(A\cup B)$.

10. (1) $A\cap B\cap C=\varnothing$. (2) $A\subseteq B\cup C$. (3) $A-B=A-C$.

13. 例如 $A=\{a\}$, $B=C=\{b\}$,则 $A\cup(B\oplus C)=A\cup\varnothing=A$. 由于 $A\cup B=A\cup C$,所以 $(A\cup B)\oplus(A\cup C)=\varnothing$,因此 $A\cup(B\oplus C)\neq(A\cup B)\oplus(A\cup C)$.

15. 设 $A_1,A_2,\cdots,A_n$ 是集合,则

$$\begin{aligned}|A_1\cup A_2\cup\cdots\cup A_n|=&\sum_{i=1}^{n}|A_i|-\sum_{1\leqslant i<j\leqslant n}|A_i\cap A_j|\\&+\sum_{1\leqslant i<j<k\leqslant n}|A_i\cap A_j\cap A_k|-\cdots\\&+(-1)^{n+1}|A_1\cap A_2\cap\cdots\cap A_n|\end{aligned}$$

16. $n!\left(1-\frac{1}{1!}+\frac{1}{2!}+\cdots+(-1)^n\frac{1}{n!}\right)$.

17. $n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$.

习题 1.5

1. 15 个不同的划分.

4. 均不成立. 例如 $A=\{a,b,c,d\}$,取 A 的划分为 $\pi_1=\{\{a\},\{b,c,d\}\}$, $\pi_2=\{\{a\},\{d\},\{b,c\}\}$.

5. (3) 将 n 个元素的集合 A 划分成 2 个块 A_1 和 A_2,先将 A 中的第一个放在第一个块 A_1 中,对于其余的 $n-1$ 个元素分别考虑是否与第一个元素在同一个块 A_1 中,只有两种情况发生: $x\in A_1$ 或 $x\notin A_1$,于是共有 $\overbrace{2\cdot 2\cdot\cdots\cdot 2}^{n-1\text{个}}=2^{n-1}$ 种放的方式,但要排除所有元素都在 A_1 中而 A_2 为空的情形. 故 $S(n,2)=2^{n-1}-1$.

6. (1) $\{A_1,A_2,A_5\}$ 是 A 的划分. (2) $\{A_1,A_3,A_5\}$ 不是 A 的覆盖. (3) $\{A_3,A_6\}$ 是 A 的划分. (4) $\{A_2,A_3,A_4\}$ 不是 A 的覆盖.

7. 共 5 个.

习题 1.6

2. 选取(0,1)开区间的一个可列子集合$\{a_0,a_1,\cdots a_n,\cdots\}$,再构造双射.

3. 令 $f:[0,1]\to[a,b]$,$f(x)=a+(b-a)x$.

4. 对于正有理数集合 $\mathbf{Q}^+=\{n/m\mid m,n\in\mathbf{N},m\neq 0,m$ 与 n 互素$\}$,令 $f:\mathbf{Q}^+\to\mathbf{N}\times\mathbf{N}$,$f(n/m)=(m,n)$,利用 $\mathbf{N}\sim\mathbf{N}\times\mathbf{N}$.

5. 在 $\mathbf{R}-\mathbf{Q}$ 中选取可列子集$\{a_0,a_1,\cdots a_n,\cdots\}$,再利用 $\mathbf{Q}$ 可列可构造双射.

6. 假设$|A|=|P(A)|$,则存在 A 到 $P(A)$的双射 f. 令 $S=\{x\mid x\notin f(x)\}$,考虑是否 $y\in S$.

习题 2.1

2. 16 个.

3. $R=\{(1,0),(2,1),(3,2),(4,3),(0,0),(2,1),(4,2)\}$.

4. 正确的有 $3\mid-12$, $-3\mid 0,0\mid 0,2\mid -2,-2\mid 2$. 不正确的有 $4\mid 6,0\mid -3$.

13. (1) $R=\{(2,2),(2,4),(2,6),(3,3),(3,6),(4,4),(5,5),(6,6)\}$.

(2) $R=\{(1,0),(2,0),(2,1),(3,1),(3,2),(4,2),(4,3),(5,3),(5,4)\}$.

(3) $R=\{(2,3),(2,5),(3,2),(3,4),(3,5),(4,3),(4,5),(5,2),(5,3),(5,4),$
$(5,6),(6,5)\}$.

(4) $R=\{(3,2),(4,2),(4,3),(5,2),(5,3),(6,2),(6,3),(6,5),(2,0),(3,0),(4,0),(5,0),(6,0)\}$.

14. (1)、(2)、(3)均不是 A 到 B 的函数.(4) 是 A 到 B 的函数.

15. (1) f 不能构成函数.(2) f 能构成 $\mathbf{R}$ 上的一个函数.

习题 2.2

1. $R\cup S=\{(0,3),(1,2),(2,1),(3,0),(0,1),(2,3)\}$,$R\cap S=\{(1,2)\}$,

$\overline{R}=A\times A-R=\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,3),(2,0),(2,2),(2,3),$
$(3,1),(3,2),(3,3)\}$.

$R-S=\{(0,3),(2,1),(3,0)\}$,$S-R=\{(0,1),(2,3)\}$,

$R\oplus S=(R-S)\cup(S-R)=\{(0,3),(2,1),(3,0),(0,1),(2,3)\}$.

3. $R^{-1}=\{(b,b),(c,b),(a,c)\}$,$S^{-1}=\{(a,b),(a,c),(d,c),(c,d)\}$,

$R\circ S=\{(b,a),(b,d)\}$,$S\circ R=\{(d,a)\}$,$R^2=R\circ R=\{(b,b),(b,c),(b,a)\}$,

$S^2=S\circ S=\{(c,c),(d,a),(d,d)\}$,$R\circ S\circ R=(R\circ S)\circ R=\varnothing$,$S\circ R^2=\varnothing$.

6. 例如,取 $A=\{a,b,c\}$,$B=\{1,2,3\}$,$C=\{\alpha,\beta,\gamma\}$,令

$S=\{(a,1),(a,2),(b,2)\}$,$T=\{(a,2),(a,3)\}$,$R=\{(1,\alpha),(2,\beta),(3,\alpha)\}$,

这时$(S\cap T)\circ R=\{(a,2)\}\circ R=\{(a,\beta)\}$,而

$$S\circ R=\{(a,\alpha),(a,\beta),(b,\beta)\},T\circ R=\{(a,\alpha),(a,\beta)\},$$

显然 $S\circ R\cap T\circ R=\{(a,\alpha),(a,\beta)\}$,所以$(S\cap T)\circ R\neq(S\circ R)\cap(T\circ R)$.

9. 对 m 归纳.

10. 由于$|A|=n$, A 上所有不同的关系共有 2^{n^2} 个,考虑关系 $R^0,R^1,R^2,\cdots,R^{2^{n^2}}$ 即可.

11. $\bigcup\limits_{n=0}^{\infty}R^n=R^0\cup R^1\cup R^2=\{(a,a),(b,b),(c,c),(d,d),(b,c),(c,a),(b,a)\}$.

12. $\mathbf{N}$ 上的关系 $R=\{(x,y)\mid y=x+1\}=\{(0,1),(1,2),(2,3),\cdots\}$及 $S=\{(x,y)\mid x=y+1\}=\{(1,0),(2,1),(3,2),\cdots\}$,这时 $R\circ S=I_N$,但 R 和 S 不是 N 上的双射.

习题 2.3

3. $R_1=\{(a,b),(b,c),(a,c)\}$,$R_2=\{(a,b),(b,c),(a,c),(b,a),(b,b),(a,a)\}$,

$R_3=\{(a,b),(b,c),(a,c),(c,b),(a,a),(b,b),(c,c)\}$.

4. (1) 取 $A=\{a,b,c\}$,A 上的关系 $R=\{(a,b),(b,c)\}$.

(2) 必要性证明用反证法.

5. (1) 取 $A=\{a,b,c\}$,A 上的关系 $R=\{(a,b),(b,c),(c,a)\}$.

6. n^2-n.

7. 逆命题不成立. 取 $A=\{a,b,c\}$,A 上的关系 $R=\{(a,a),(a,b),(b,b)\}$.

8. R 具有自反性、反对称性和传递性.

9. $\backsim$具有自反性、对称性和传递性.

10. 当$|X|=1$ 时,则 $R=\{(X,X)\}$具有对称性、反对称性和传递性. 当$|X|\geqslant 2$ 时,R 具有对称性.

11. $R=\{(a,a),(b,a),(a,b),(b,c)\}$.

12. (1) 真. (2) 真. (3) 真. (4) 假. (5) 假.

习题 2.4

2. $r(R)=R\cup I_A=\{(a,a),(a,b),(b,a),(b,c),(c,d),\underline{(b,b),(c,c),(d,d)}\}$,

$s(R)=R\cup R^{-1}=\{(a,a),(a,b),(b,a),(b,c),(c,d),\underline{(c,b),(d,c)}\}$,

$t(R)=\{(a,a),(a,b),(b,a),(b,c),(c,d),\underline{(b,b),(a,c),(b,d),(a,d)}\}$.

4. 根据传递闭包的定义并注意到:对于任意 $x,y\in\mathbf{Z}$,若 $x<y$,则存在正整数 m 使得 $y=x+m$.

7. 设 $R_1\subseteq A\times A$,$R_2\subseteq A\times A$,则下面结论成立.

(1) $r(R_1\cap R_2)=r(R_1)\cap r(R_2)$.

(2) $s(R_1\cap R_2)\subseteq s(R_1)\cap s(R_2)$.

(3) $t(R_1\cap R_2)\subseteq t(R_1)\cap t(R_2)$.

9. (1) 例如 $A=\{a,b,c\}$,$R=\{(a,b),(b,a)\}$,则 R 是反自反的,而

$r(R)=\{(a,b),(a,a),(b,b),(c,c)\}$ 和 $t(R)=\{(a,b),(b,a),(a,a),(b,b)\}$

都不具有反自反性.

(2) 例如 $A=\{a,b,c\}$,$R=\{(a,b),(b,c),(c,a)\}$,则 R 是反对称的,而

$$s(R)=\{(a,b),(b,c),(c,a),(b,a),(c,b),(a,c)\} \text{ 和}$$

$$t(R)=\{(a,b),(b,c),(c,a),(a,c),(b,a),(a,a),(b,b),(c,c),(c,b)\}$$

都不具有反对称性.

10. $rt(R)=\{(a,b),(b,c),(a,c),(a,a),(b,b),(c,c)\}$.

习题 2.5

5. (1) 若$|X|\leqslant 1$,R 是 A 上的等价关系. 若$|X|\geqslant 2$,R 是自反的和对称的,但不传递.

(2) R 是 A 上的等价关系.

6. 例如 $A=\{a,b,c\}$,取

$$R=\{(a,b),(b,a)\}\cup I_A,\quad S=\{(b,c),(c,b)\}\cup I_A,$$

这时 R 和 S 是集合 A 上的等价关系.

7. 最小的包含 R 的等价关系为

$$tsr(R)=\bigcup_{i=0}^{\infty}(R\cup R^{-1})^i=I_A\cup(R\cup R^{-1})\cup(R\cup R^{-1})^2\cup\cdots$$

8. (2) $A/R=\{\{a,c\},\{b,d\}\}$.

12. 集合 A 的所有的等价关系个数为 15 .

13. 集合 A 的划分 $A/(R_1\cap R_2)$ 是两个集合 A 的划分 A/R_1 和 A/R_2 的交叉划分.

16. 只要 R 具有自反性和传递性,则 S 是集合 A 上的等价关系.

习题 2.6

1. (4) 由 R 产生的所有极大相容类有 4 个,分别为{set, function, operation, relation}, {operation, relation, logic, algebra, graph}, {set, operation, relation, algebra},{function, operation, relation, logic}.

2. (1) $R\cup R^{-1}\cup I_A=\{(1,4),(4,1),(2,5),(5,2),(1,1),(2,2),(3,3),(4,4),(5,5)\}$.

(2) A 关于 $R\cup R^{-1}\cup I_A$ 的所有极大相容类分别为$\{1,4\}$, $\{2,5\}$和$\{3\}$.

3. (2) 当$\{A_i\mid i\in I\}$是集合 A 的划分时,$R=\bigcup_{i\in I}A_i\times A_i$ 是 A 上的等价关系 .

5. (3) $A=\{a,b\}$,$R=\{(a,a),(b,b)\}$.

(4)和(5)$A=\{a,b\}$,取 $R=A\times A$ 及 $S=\{(a,a),(b,b)\}$.

(7) $A=\{a,b,c\}$,取 $R=\{(a,b),(b,a)\}\cup I_A$ 及 $S=\{(b,c),(c,b)\}\cup I_A$.

习题 2.7

1. $A=\{1,2,3,4,6,12\}$,$\mathrm{COV}(A)=\{(1,2),(1,3),(2,4),(2,6),(3,6),(4,12),(6,12)\}$.

2. $\mathrm{COV}(A)=\{(a,b),(b,c),(a,d),(d,e),(c,e)\}$.

5. (1)(3)(4)(5)$A=\{a,b\}$,$R=\{(a,a),(b,b),(a,b)\}$,$S=\{(a,a),(b,b),(b,a)\}$.

(7) $A=\{a,b,c\}$,$R=\{(a,b),(a,c)\}\cup I_A$,$S=\{(b,a),(b,c)\}\cup I_A$.

8. (1) 集合 A 的最大元素为 a,最小元素不存在,极大元素为 a,极小元素为 d 和 e.

(2) 子集$\{b,c,d\}$的上界为 a,下界为 d,上确界为 a,下确界为 d.

11. (2) $(F(\mathbf{N}),\subseteq)$无极大元. (3) $\varnothing$是$(F(\mathbf{N}),\subseteq)$的极小元. (4) $\sup\{A,B\}=A\cup B$. (5) $\inf\{A,B\}=A\cap B$.

12. $(A,\subseteq)$的极小元为$\{x\}$,其中 x 为 S 中任意元素;极大元为 $S-\{x\}$,其中 x 为 S 中任意元素;没有最小元素;没有最大元素.

13. (2) (B^A,R)存在最大元的必要条件是偏序集$(B,\leqslant)$存在最大元 M. 最大元$F\in B^A$的一般形式为 $F(x)=M$, $\forall x\in A$,其中 M 为偏序集$(B,\leqslant)$的最大元.

习题 3.1

1. (1)(2)(4)(6)(7)是命题,真值为 1.

(3) 不是命题,因为 x 和 y 的取值未定,于是无法确定"$x>y$"的真值.

(5) 是命题,真值为 0.

2. (1) p:我去游泳.

(2) p：张三看书，q：张三听 MP4 音乐.
(3) p：小李能歌，q：小李善舞.
(4) p：这学期我选修人工智能课程，q：这学期我选修模式识别课程.
(5) p：明天去深圳的飞机是上午八点起飞，q：明天去深圳的飞机是上午八点半起飞.
(6) p：我有时间，q：我回家去看望我的父母.
(7) p：我今天进城，q：天下雨.
(8) p：小张外出，q：小张上网，r：他睡觉.
(9) p：你刻苦学习，q：你取得好成绩.
(10) p：你走，q：我留下值班.

习题 3.2

1. (1) $\neg p$：现在不是很多人都有车.
(2) "-2 是偶数或 3 是正数"的否定命题为"-2 不是偶数并且 3 不是正数".
(3) $p \vee \neg p$：每个自然数都是整数或者不是每个自然数都是整数.
2. $p \wedge q$：今明两天都有雨.
$p \vee q$：今天或者明天有雨.
$p \rightarrow q$：如果今天有雨，那么明天有雨.
$p \oplus q$：今明两天只有一天有雨.
$p \uparrow q$：不可能今明两天都有雨.
$p \downarrow q$：不可能今天或明天有雨.
$p \overset{n}{\rightarrow} q$：不可能今天有雨，则明天有雨.
3. $\neg(p \wedge q)$：我们不能既去图书馆又去上网.
4. $\neg p \wedge \neg q$.
5. "张红和张兰是姐妹"中的和表示的是两个人之间的关系，而联结词 $\wedge$ 表示的是两个命题之间的"和".
6. 用 p:今天体育课考试，q:今天下雨，r:马老师来了，则 $p \leftrightarrow (\neg q \wedge r)$ 表示"今天体育课考试当且仅当今天不下雨并且马老师来了".

习题 3.3

1. (1) 令 p：a 是奇数，q：b 是奇数，r：$a+b$ 是偶数，所以 $p \wedge q \rightarrow r$.
(2) 令 p：正整数 $n \leqslant 2$ 时，q：不定方程 $x^n + y^n = z^n$ 有正整数解，所以 $q \rightarrow p$.
(3) 令 p：天在下雨，q：我去书店，所以 $p \wedge \neg q$.
(4) 令 p：两矩阵相等，q：两矩阵对应的元素分别相等，所以 $p \leftrightarrow q$.
(5) 令 p：这苹果甜，q：我打算买，所以 $p \wedge \neg q$.
(6) 令 p：我接到正式邀请，q：我去参加圣诞晚会，所以 $\neg p \rightarrow \neg q$.
(7) 令 p：我和小王是同学，所以 p.
(8) 令 p：他看今晚的 NBA 篮球比赛，q：他来上自习，所以 $p \wedge \neg q$.
(9) 令 p：她学习成绩好，q：她的动手能力很强，所以 $\neg p \wedge q$.
(10) 令 p：我的手机没电了，q：借你的手机用一下，所以 $p \wedge q$.
3. (1) 永真式，利用真值表可知.
(2) 中性式，分别考虑 $p=0, q=1, r=1$ 和 $p=0, q=0, r=0$.

(3) 中性式,分别考虑 $p=0,q=0,r=0$ 和 $p=1,q=1,r=0$.

(4) 中性式,分别考虑 $p=1,q=1,r=1,s=1$ 和 $p=0,q=0,r=0,s=0$.

4. (1) 由 $B\rightarrow A$ 取 0 得出 $A=0$.

(2) 利用真值表及代入定理.

(3) 由 $B\rightarrow A$ 取 0 推出 $\neg A\rightarrow\neg B$ 取 0.

5. 利用真值表及代入定理.

6. (1) 由 $A\rightarrow B$ 取 0 推出 $A\rightarrow B$ 取 0.

(2) 若 $(A\vee B)\wedge(A\rightarrow C)\wedge(B\rightarrow C)\rightarrow C$ 为 0 可得出矛盾.

(3) 由 $\neg A$ 取 0 推出 $(A\rightarrow B)\wedge(A\rightarrow\neg B)=0$.

(4) 由 $\neg A\rightarrow B$ 取 0 得出 $A=0$.

习题 3.4

3. (1) 不成立. 取 $A=p,B=p\vee q,C=p$.

(2) 不成立. 取 $A=p,B=p\wedge q,C=p$.

(3) 成立. 因为 $\neg A=\neg B$,所以 $\neg\neg A=\neg\neg B$,于是 $A=B$.

4. 利用真值表法进行证明.

5. (1)(3)(4)用等值演算法,(2)用真值表法.

6. (1) $\neg A=\neg(A\wedge A)=A\uparrow A$.

(2) $A\wedge B=\neg(\neg(A\wedge B))=\neg(A\uparrow B)=(A\uparrow B)\uparrow(A\uparrow B)$.

(3) $A\vee B=\neg(\neg A\wedge\neg B)=(\neg A)\uparrow(\neg B)=(A\uparrow A)\uparrow(B\uparrow B)$.

7. (1) $\neg A=\neg(A\vee A)=A\downarrow A$.

(2) $A\wedge B=\neg(\neg A\vee\neg B)=(\neg A)\downarrow(\neg B)=(A\downarrow A)\downarrow(B\downarrow B)$.

(3) $A\vee B=\neg(\neg(A\vee B))=\neg(A\downarrow B)=(A\downarrow B)\downarrow(A\downarrow B)$.

8. (1)、(2)用真值表法. (3)、(4)用等值演算法.

9. (1) $A\wedge C=(A\downarrow A)\downarrow(C\downarrow C)$.

(2) $A\vee B=(A\downarrow B)\downarrow(A\downarrow B)$.

(3) $\neg(A\wedge(B\vee C))=((A\downarrow A)\downarrow(B\downarrow C))\downarrow((A\downarrow A)\downarrow(B\downarrow C))$.

(4) B.

10. (1) 永假式. (2) 中性式.

12. $(p\oplus q)^*=(p\wedge q)\vee(\neg p\wedge\neg q)=p\odot q$.

习题 3.5

1. (1) $p\wedge q$(析取范式和合取范式).

(2) $(\neg p\vee\neg q)\wedge(p\vee q)$(合取范式),$(\neg p\wedge q)\vee(p\wedge\neg q)$(析取范式).

(3) $p\vee\neg q\vee r$(析取范式和合取范式).

(4) $(p\wedge\neg q)\vee r$(析取范式),$(p\vee r)\wedge(\neg q\vee r)$(合取范式).

2. 王教授是上海人.

3. 当只有 1 人成绩最好时,是 p;当有 2 人成绩并列最好时,应是 p,s 或 p,r.

4. 应派 p 和 s 参加围棋比赛.

5. (1) $(p\wedge q)\vee(\neg p\wedge q)\vee(p\wedge\neg q)$(主析取范式),$(p\vee q)$(主合取范式),中性式.

(2) 主析取范式不存在,$(p\vee q)\wedge(p\vee\neg q)\wedge(\neg p\vee q)\wedge(\neg p\vee\neg q)$(主合取范式),

永假式.

(3) $(p\wedge q\wedge r)\vee(p\wedge\neg q\wedge r)\vee(p\wedge\neg q\wedge\neg r)\vee(\neg p\wedge q\wedge r)\vee(\neg p\wedge\neg q\wedge r)$(主析取范式),$(p\vee q\vee r)\wedge(p\vee\neg q\vee r)\wedge(\neg p\vee\neg q\vee r)$(主合取范式),中性式.

(4) $(p\wedge q\wedge r)\vee(\neg p\wedge\neg q\wedge\neg r)$(主析取范式),

$(\neg p\vee q\vee r)\wedge(\neg p\vee q\vee\neg r)\wedge(\neg p\vee\neg q\vee r)\wedge$

$(p\vee\neg q\vee r)\wedge(p\vee\neg q\vee\neg r)\wedge(p\vee q\vee\neg r)$(主合取范式),中性式.

6. 原式$=(\neg p\vee q\vee r)\wedge(\neg p\vee\neg q\vee r)\wedge(p\vee\neg q\vee r)$,中性式.

7. 主析取范式均为$(p\wedge q\wedge r)\vee(p\wedge q\wedge\neg r)\vee(\neg p\wedge q\wedge r)\vee(\neg p\wedge\neg q\wedge r)$.

8. $A=(p\wedge\neg q\wedge r)\vee(\neg p\wedge q\wedge r)\vee(\neg p\wedge q\wedge\neg r)$.

9. $F=(p\wedge r)\vee(q\wedge r)=(p\wedge q\wedge r)\vee(p\wedge\neg q\wedge r)\vee(\neg p\wedge q\wedge r)$(主析取范式),

$F=(\neg p\vee\neg q\vee r)\wedge(\neg p\vee q\vee r)\wedge(p\vee\neg q\vee r)$

$\wedge(p\vee q\vee\neg r)\wedge(p\vee q\vee r)$(主合取范式).

10. $F=(\neg p\wedge\neg q\wedge r)\vee(\neg p\wedge q\wedge r)\vee(p\wedge\neg q\wedge\neg r)\vee(p\wedge q\wedge\neg r)$,

$F=(p\vee q\vee r)\wedge(p\vee\neg q\vee r)\wedge(\neg p\vee q\vee\neg r)$

$\wedge(\neg p\vee\neg q\vee\neg r)$(主合取范式).

习题 3.6

3. 利用$\{\neg,\wedge,\vee\}$是功能完备的联结词集.

5. (1) 对于只含有联结词$\{\neg,\leftrightarrow\}$的任意命题公式 A,使 A 的真值为 1 的所有真值指派的个数为偶数.

(2) 利用(1)及 $p\leftrightarrow q=\neg(p\oplus q)$.

(3) 类似于书上例子.

习题 3.7

3. 推理形式 $p\to q,q\Rightarrow p$ 是无效的.

10. (1) 只需证明 $A\to B\Rightarrow(A\to(B\to C))\to(A\to C)$.

(2) 只需证明 $A\to B,A\to\neg B\Rightarrow\neg A$.

11. $p\to q\vee r,s\to\neg r,p\wedge s\Rightarrow q$.

12. 小东爸爸的意思是:$q\to p$ 且 $q\to r$;小东理解为:$p\to q$ 且 $q\to r$.

习题 4.1

1. $D_1=\{1,2,3,4,5\}$,$D_2=\mathbf{N}$,$D_3=$全域.

2. (1) $D=\mathbf{Z}$,$Q(x)$:x 是有理数.

(2) $D=\mathbf{R}$,$Q(x)$:x 是有理数,$Z(x)$:x 是整数.

3. (1) a:小赵,$W(x)$:x 是工人.

(2) a:张三,b:李四,$I(x,y)$:x 是 y,$f(x)$:x 的父亲.

(3) a:-3,$Q(x)$:x 是有理数.

(4) a:米卢,$L(x)$:x 喜欢踢足球.

(5) $Q(x)$:x 是有理数,$R(x)$:x 是实数,全称量词 $\forall$.

(6) $Q(x)$:x 是有理数,$R(x)$:x 是实数,存在量词 $\exists$.

(7) a:北京,$H(x)$:x 举办 2008 年奥运会.

(8) $E(x)$:x 锻炼身体,全称量词 $\forall$.

4. (1) $\forall x \exists y E(x,y)$：班上所有同学都选修了一些计算机课程.

(2) $\forall x \forall y E(x,y)$：班上所有同学都选修了所有的计算机课程.

(3) $\exists x \exists y E(x,y)$：班上有些同学选修了一些计算机课程.

(4) $\exists x \forall y E(x,y)$：班上有些同学选修了所有计算机课程.

(5) $\forall y \exists x E(x,y)$：所有的计算机课程都有同学选修.

(6) $\forall y \forall x E(x,y)$：所有的计算机课程被每个同学选修了.

(7) $\exists y \exists x E(x,y)$：有些计算机课程都有同学选修.

(8) $\exists y \forall x E(x,y)$：有的计算机课程被所有同学选修.

5. (1) $\forall x$ 的辖域为 $P(x) \vee \exists y R(y)$，$\exists y$ 的辖域为 $R(y)$. 在 $P(x) \vee \exists y R(y)$ 中的个体变元 x 是约束变元，$R(y)$ 中的 y 是约束变元，$Q(x)$ 中的 x 是自由变元.

(2) $\forall x$ 的辖域为 $\exists y(P(x,y) \wedge Q(y,z))$，$\exists y$ 的辖域为 $P(x,y) \wedge Q(y,z)$，$\exists x$ 的辖域为 $P(x,y)$. 个体变元 x 在 $P(x,y) \wedge Q(y,z)$ 和 $P(x,y)$ 中的出现均为约束变元，$P(x,y) \wedge Q(y,z)$ 中个体变元 y 为约束变元，z 是自由变元，$P(x,y)$ 中的 y 是自由变元.

(3) 第一次出现的 $\forall x$ 的辖域为 $P(x) \wedge \exists x Q(x)$，$\exists x$ 的辖域为 $Q(x)$，而第二次出现的 $\forall x$ 的辖域为 $P(x)$. 个体变元 x 的最后一次出现为自由变元，别的出现均为约束变元.

(4) $\forall x$ 的辖域为 $\forall y(R(x,y) \vee L(z,y))$，$\forall y$ 的辖域为 $R(x,y) \vee L(z,y)$，$\exists x$ 的辖域为 $S(x,y)$. 出现在 $R(x,y) \vee L(z,y)$ 和 $S(x,y)$ 中的个体变元 x 均为约束变元，出现在 $R(x,y) \vee L(z,y)$ 中的个体变元 y 均为约束变元，而 z 是自由变元，出现在 $S(x,y)$ 中的个体变元 y 为自由变元.

6. $\exists x P(x) \wedge \exists x Q(x) = \exists x P(x) \wedge \exists y Q(y)$.

7. $\forall x(P(x,y) \wedge \exists y Q(x,y)) = \forall x(P(x,t) \wedge \exists y Q(x,y))$.

习题 4.2

1. (1) 令 a：小李，$S(x)$：x 是学生，$T(x)$：x 是老师，所以 $\neg S(a) \wedge T(a)$.

(2) 用 $P(x)$：x 是人，$M(x)$：x 犯错误，所以 $\forall x(P(x) \to M(x))$.

(3) 令 $S(x)$：x 是大学生，$T(x)$：x 是体育爱好者，所以 $\exists x(S(x) \wedge T(x))$.

(4) 令 $T(x)$：x 是老虎，$E(x)$：x 要吃人，所以 $\forall x(T(x) \to E(x))$.

(5) 用 $G(x)$：x 是研究生，$R(x)$：x 科研人才，所以 $\neg \forall x(G(x) \to R(x))$.

(6) 设 $Z(x)$：x 是整数，$E(x)$：x 偶数，$O(x)$：x 奇数，所以 $\forall x(Z(x) \to (E(x) \vee O(x)))$.

(7) 用 $S(x)$：x 是大学生，$T(x)$：x 是老师，$A(x,y)$：x 钦佩 y，所以 $\forall x \exists y(S(x) \wedge T(y) \to A(x,y))$.

(8) 令 $S(x)$：x 是大学生，$L(x)$：x 喜欢《超级女声》节目，所以 $\exists x(S(x) \wedge \neg L(x))$.

(9) 令 a：姚明，b：杨利伟，$P(x)$：x 是 NBA 球员，$M(x)$：x 去过太空，所以 $P(a) \wedge M(b)$.

(10) 设 $C(x)$：x 是猫，$M(x)$：x 老鼠，$W(x)$：x 白的，$B(x)$：x 是黑的，$G(x)$：x 好的，$A(x,y)$：x 抓住 y，所以 $\forall x \forall y(C(x) \wedge (W(x) \vee B(x)) \wedge M(y) \wedge A(x,y) \to G(x))$.

2. 令 $E(x)$：x 是专家，$T(x)$：x 是教师，$Y(x)$：x 是青年人，则所给命题分别符号化为：

(1) $\forall x(E(x) \wedge T(x))$.

(2) $\exists x Y(x)$.

(3) $\exists x(Y(x) \wedge E(x))$.

3. 令 $Z(x)$：x 是整数，$N(x)$：x 是自然数，$Q(x)$：x 是有理数，则所给命题分别符号化为：

(1) $\forall x(N(x)\rightarrow Z(x))$.

(2) $\forall x(Z(x)\rightarrow Q(x))$.

(3) $\exists x(Z(x)\land\neg N(x))$.

(4) $\exists x(Q(x)\land\neg Z(x))$.

(5) $\forall x(N(x)\rightarrow Q(x))\land\exists x(Q(x)\land\neg N(x)\land\neg Z(x))$.

4. 令 $W(x)$：x 喜欢步行，$C(x)$：x 喜欢坐车，$B(x)$：x 喜欢骑自行车，则所给命题分别符号化为：

(1) $\forall x(W(x)\rightarrow\neg C(x))$.

(2) $\forall x(B(x)\lor C(x))$.

(3) $\neg\forall xC(x)$.

(4) $\exists x\neg W(x)$.

5. 令 $A(x)$：x 是动物，$C(x)$：x 是牛，$H(x)$：x 有角，则所给命题分别符号化为：

(1) $\forall x(C(x)\rightarrow H(x))$.

(2) $\exists x(A(x)\land C(x))$.

(3) $\exists x(A(x)\land H(x))$.

6. 令 $B(x)$：x 是鸟，$F(x)$：x 会飞，$M(x)$：x 是猴子，则所给命题分别符号化为：

(1) $\forall x(B(x)\rightarrow F(x))$.

(2) $\forall x(M(x)\rightarrow\neg F(x))$.

(3) $\forall x(M(x)\rightarrow\neg B(x))$.

7. 令 $S(x)$：x 是学生，$D(x)$：x 是勤奋的，$C(x)$：x 是聪明的，$H(x)$：x 是有所作为的，则所给命题分别符号化为：

(1) $\forall x(S(x)\rightarrow D(x)\lor C(x))$.

(2) $\forall x(D(x)\rightarrow H(x))$.

(3) $\neg\forall x(S(x)\rightarrow H(x))$.

(4) $\exists x(S(x)\land C(x))$.

8. 令 $B(x)$：x 是桌上的书，$M(x)$：x 是杰作，$T(x)$：x 是天才，$P(x)$：x 是人，$F(x)$：x 是不出名的，$W(x,y)$：x 写 y，则所给命题分别符号化为：

(1) $\forall x(B(x)\rightarrow M(x))$.

(2) $\forall x\forall y(P(x)\land M(y)\land W(x,y)\rightarrow T(x))$.

(3) $\exists x\exists y(P(x)\land F(x)\land B(y)\land W(x,y))$.

(4) $\exists x(P(x)\land F(x)\land T(x))$.

9. 令 $R(x)$：x 是兔子，$T(x)$：x 是乌龟，$F(x,y)$：x 比 y 跑得快，则所给命题分别符号化为：

(1) $\forall x\forall y(R(x)\land T(y)\rightarrow F(x,y))$.

(2) $\exists x\forall y(R(x)\land T(y)\rightarrow F(x,y))$.

(3) $\neg\forall x\forall y(R(x)\land T(y)\rightarrow F(x,y))$.

(4) $\neg\exists x\exists y(R(x)\land R(y)\land F(x,y)\land F(y,x))$.

10. 令 $G(x)$：x 是金子，$L(x)$：x 是闪光的，则所给命题分别符号化为：

$$\forall x(G(x) \to L(x)) \wedge \neg \forall x(L(x) \to G(x))$$

习题 4.3

2. (1) 0.(2) 1.(3) 0.

3. (1) 0.(2) 1.

4. (1) 1.(2) 1.(3) 0.(4) 0.

习题 4.4

8. (1) 成立.(2) 成立.

习题 4.5

1. (1)(2)(4)不是.(3)(5)是.

2. (1) $\forall x \exists y(\neg A(x) \vee B(x,y))$.(2) $\exists x \exists y \forall z(P(x,y) \vee \neg Q(z) \vee R(x))$.

(3) $\forall x \forall y \exists z(A(x) \wedge \neg B(y,z))$.(4) 1.

3. (1) $\forall x \forall y \forall z((\neg A(x) \vee B(y)) \wedge (\neg A(t) \vee C(z)))$.

(2) $\forall x \exists y \forall z(\neg A(x) \vee \neg B(z) \vee C(x,y))$.

(3) $\forall x \exists y \exists z \forall u \forall v(\neg A(x,y,v) \vee B(x,z) \vee C(x,u,z))$.

(4) $\forall x \forall y \exists v \forall z \forall u(\neg A(x,y,z) \vee \neg B(x,u) \vee B(y,v))$.

习题 4.6

3. 对于个体域 D 上的任意解释 I，若 $\forall x(A(x) \vee B(x))=0$，推出 $\forall xA(x) \vee \forall xB(x)=0$.

4. 在个体域 D 上任意作解释 I，若 $\forall x(A(x) \to B(x))=0$，则推出 $\exists xA(x) \to \forall xB(x)=0$.

5. (1)(2)均不是永真式.

6. (1)(2)不成立.

习题 5.1

2. 答案如表 C-2 所示.

表 C-2

集合 \ 运算	$+$	$-$	$\cdot$	$\|x-y\|$	$\|x\|$	max	min
$\mathbf{Z}$	√	√	√	√	√	√	√
$\mathbf{N}$	√	×	√	√	√	√	√
$\{x\|0 \leqslant x \leqslant 10\}$	×	×	×	√	√	√	√
$\{x\| \|x\| \leqslant 5\}$	×	×	×	×	√	√	√
$\{2x\|x \in \mathbf{Z}\}$	√	√	√	√	√	√	√

7. 令 $\varphi: \mathbf{R}^+ \to \mathbf{R}, \varphi(x)=\ln x, \forall x \in \mathbf{R}^+$.

8. $(\mathbf{R}^*, \cdot)$与$(\mathbf{R}, +)$不可能同构.

若 φ 是$(\mathbf{R}^*, \cdot)$与$(\mathbf{R}, +)$的同构映射，则因为 0 是$(\mathbf{R}^*, \cdot)$的幺元且 1 是$(\mathbf{R}, +)$的幺元，于是 $\varphi(1)=0$. 设 $\varphi(-1)=y$.

一方面,因为 $1\neq-1$ 且 φ 是双射,则 $y\neq0$.

另一方面,$0=\varphi(1)=\varphi((-1)\cdot(-1))=\varphi(-1)+\varphi(-1)=y+y$,于是 $y=0$,这与 $y\neq0$ 矛盾. 故 $(\mathbf{R}^*,\cdot)$ 与 $(\mathbf{R},+)$ 不可能同构.

习题 5.2

2. 由于 $\boldsymbol{E}=\mathrm{diag}(1,1,\cdots,1)\in\boldsymbol{M}_n(\mathbf{R})$ 是 $\boldsymbol{M}_n(\mathbf{R})$ 关于矩阵的乘法运算 $\cdot$ 的单位元素,而对于 n 阶零矩阵 $\mathbf{0}$,不存在任何 $A\in\boldsymbol{M}_n(\mathbf{R})$ 满足 $\mathbf{0}\cdot\boldsymbol{A}=\boldsymbol{A}\cdot0=\boldsymbol{E}$,即 n 阶零矩阵 $\mathbf{0}$ 关于矩阵的乘法运算 $\cdot$ 无逆元,故 $(\boldsymbol{M}_n(\mathbf{R}),\cdot)$ 不能构成群.

3. $(\mathbf{Z}_6,-\{0\},\cdot_6)$ 不是群,$(\mathbf{Z}_m-\{0\},\cdot_m)$ 是群的充要条件是 m 是素数.

4. x 关于 $*$ 存在逆元 $4-x$.

6. 对于任意 $x\in G$,$x^{-1}=x$.

9. 对于任意 $x\in G$,因为 $(x^{-1})^{-1}=x$,所以 x 和 x^{-1} 在群 G 中是成对出现的. 显然 $e\cdot e=e$,即 $e=e^{-1}$. 如果对于任意 $x\neq e$ 均有 $x\cdot x\neq e$,即 $x\neq x^{-1}$,则 $|G|$ 是奇数,与已知矛盾.

10. 首先证明:对于任意 $x,y,z\in G$,若 $x\cdot y=x\cdot z$,则 $y=z$. 再证明:e 也是 $(G,\cdot)$ 的右单位元. 最后证明:$\hat{x}$ 也是 x 的右逆元.

11. (1) G 关于映射的复合运算 $\circ$ 是封闭的,且若 $f(x)=ax+b$,则 $f^{-1}(x)=\dfrac{1}{a}x+\left(-\dfrac{b}{a}\right)$.

12. (1) $(x,y)\in G$ 有逆元 $\left(\dfrac{1}{x},-\dfrac{y}{x}\right)\in G$.

习题 5.3

4. $(R,+,\circ)$ 不能构成环,因为函数的复合运算 $\circ$ 对函数的加法运算 $+$ 不可分配.

8. 对于任意 $0\neq a+b\mathrm{i}\in R$,$a,b\in\mathbf{Q}$,$\dfrac{a}{a^2+b^2}-\dfrac{b}{a^2+b^2}\mathrm{i}\in R$.

9. $(x,0)\in R(x\neq0)$ 和 $(0,y)\in R(y\neq0)$ 是环 $(R,+,\cdot)$ 的所有零因子.

11. (1) 对于任意 $x\in R$,考虑 $(x+x)\cdot(x+x)$.

(2) 对于任意 $x\in R$,考虑 $(x+y)\cdot(x+y)$.

(3) 若 $(R,+,\cdot)$ 不是含幺元,当然 $(R,+,\cdot)$ 不是整环. 若 $(R,+,\cdot)$ 是含幺环,其幺元为 1,由于 $|R|>2$,必存在 $a\in R$,$a\neq0,1$. 由于 $a\cdot(a-1)=a\cdot a-a=0$,所以 a 和 $a-1$ 是环 $(R,+,\cdot)$ 的零因子,因此 $(R,+,\cdot)$ 不是整环.

14. (1) -1 是 R 关于 $\oplus$ 的单位元素,$-x-2$ 是 x 关于 $\oplus$ 的逆元素,0 是 R 关于 $\odot$ 的单位元.

15. $(F,+,\cdot)\cong(\mathrm{Z}_3,+_3,\cdot_3)$.

习题 5.4

1. (a) 不是格,虽然 $\{a,c\}$ 有下界 b 和 d,但 $\{a,c\}$ 无下确界.

(b) 是格,因为其任意两个元素均有上确界以及下确界.

2. 对于任意 $x,y\in\mathbf{Z}^+$,有 $\sup\{x,y\}=[x,y]$ 且 $\inf\{x,y\}=(x,y)$.

3. 因为 $2|-2$ 且 $-2|2$,而 $2\neq-2$,所以 $\mathbf{Z}$ 关于整除关系 $|$ 不具有反对称性.

对于任意 $x,y\in\mathbf{Z}$,有 $\sup\{x,y\}=\max\{x,y\}$ 且 $\inf\{x,y\}=\min\{x,y\}$.

4～6. 多次利用“下界≤下确界”.

7. 对于任意 $x, y \in I$,则 $a \leqslant x \leqslant b$ 且 $a \leqslant y \leqslant b$,这时 $a \leqslant x \cdot y \leqslant b$ 且 $a \leqslant x + y \leqslant b$.

11. $(\mathbf{R}, \leqslant)$是链.

15. $(D_{12}, |)$不是有补格,而$(D_{15}, |)$是有补格.

17. (1) x. (2) z. (3) $\overline{x \cdot y}$. (4) $\overline{y}(z+x)$.

习题 6.1

1. 能得出任意 6 个人中有 3 个人相互认识或相互不认识的结论.

2. 将每个同学分别作为一个节点,如果两个人握过一次手就在相应的两个节点之间画一条无向边,于是得到一个无向图.

3. 将联欢舞会上的每个人分别作为一个节点,若两个人跳过一次舞,则在相应的两个节点之间画一条无向边,于是得到一个无向图.

4. 将该组里的一个人看作一个节点,若两个人是朋友,则在相应的两个节点之间连一条无向边,于是得到一个无向图.

5. 将 3 户人家分别看作 3 个节点且将 3 口井分别看作另外 3 个节点,若 1 户人家与 1 口井之间有一条路,则在该户人家与该口井对应的节点之间连一条无向边,这样就得到一个无向图.

6. 不妨认为从北岸到南岸,则在北岸可能出现的状态为 $2^4=16$ 种,其中安全状态有下面 10 种:(人,狼,羊,菜),(人,狼,羊),(人,狼,菜),(人,羊,菜),(人,羊),($\varnothing$),(菜),(羊),(狼),(狼,菜).

现将北岸的 10 种安全状态看作 10 个节点,而渡河的过程则是状态之间的转移,这样就得到一个无向图.

第 1 种:(人,狼,羊,菜)→(狼,菜)→(人,狼,菜)→(狼)→(人,狼,羊)→(羊)→(人,羊)→($\varnothing$).

第 2 种:(人,狼,羊,菜)→(狼,菜)→(人,狼,菜)→(菜)→(人,羊,菜)→(羊)→(人,羊)→($\varnothing$).

7. 用(B,C)表示 B, C 两个油桶的状态,由于 $B=0,1,2,3,4,5$ 且 $C=0,1,2,3$,于是所有状态共 $6\times4=24$ 种.

现将这 24 种状态看作 24 个节点,两节点之间连一条无向边当且仅当这两种状态可以相互转换,于是得到一个无向图.

有两种将油平分的方案:

第 1 种:$(0,0)\to(0,3)\to(3,0)\to(3,3)\to(5,1)\to(0,1)\to(1,0)\to(1,3)\to(4,0)$.

第 2 种:$(0,0)\to(5,0)\to(2,3)\to(2,0)\to(0,2)\to(5,2)\to(4,3)\to(4,0)$.

9. $n(n-1)/2-m$.

习题 6.2

2. 4.

3. (1) 设 G 是 3-正则(n,m)图,根据握手定理有 $3\cdot n=2m$. 由于 $2|2m$,因此 $2|n$,即 n 为偶数.

4. 设 $G=(V,E)$是 n 阶竞赛图,则其边数为 $|E|=n(n-1)/2$ 且对于任意 $v\in V$ 有 $\deg^+(v)+\deg^-(v)=n-1$. 根据竞赛图的定义知:

$$\sum_{v\in V}\deg^+(v)=\sum_{v\in V}\deg^-(v)=|E|=n(n-1)/2$$

8. G 至少有 7 个节点，G 的度数序列为 4，4，3，3，2，2，2，最大度 $\Delta(G)=4$ 和最小度 $\delta(G)=2$.

9. 必要性是显然的. 由于 $\sum_{i=1}^{n} d_i \equiv 0 \pmod 2$，于是 d_i 为奇数的个数是偶数. 对于任意 $i(1\leqslant i\leqslant n)$，若 $d_i=2k$，则在节点 v_i 处作 k 个环，若 $d_i=2k+1$，则在节点 v_i 处先作 k 个环，由于 d_i 为奇数的个数是偶数，进而可以配对用一条无向边连接，这样就得到一个图 G，其度数序列为 $d_1,d_2,\cdots,d_n$.

习题 6.3

1. 7 个.

2. (5,3)简单无向图的度数序列分别为：(1) 3，1，1，1，0；(2) 2，2，2，0，0；(3) 2，2，1，1，0；(4) 2，1，1，1，1.

3. (4,3)简单图的度数序列分别为：(1) 3，1，1，1；(2) 3，2，1，0；(3) 2，2，1，1.

5. 观察(a)和(b)的度为 3 的节点，与其邻接的节点都有 3 个，这 3 个节点在(a)中只有 1 个节点度数为 2，但在(b)中有 2 个节点度数为 2，所以(a)与(b)不同构.

6. 观察每个节点的出度和入度.

8. 分别考虑所有 3 阶不同构的简单无向图即可.

习题 6.4

1. 在(a)中包含所有边的轨迹为：2345215，在(b)中包含所有边的轨迹为：126534523614.

2. (1) $\sum_{l=3}^{n} C_n^l \cdot \frac{1}{2}(l-1)!$. (2) $\sum_{i=1}^{n-2} C_{n-2}^i \cdot i!$. (3) $\sum_{i=1}^{n-2} C_{n-2}^i \cdot i!+1$.

3. (1) (a) $ABCF$；(b) $ABCEF$；(c) $ABEF$；(d) $ABECF$；(e) $ADEF$；(f) $ADECF$；(g) $ADEBCF$.

(2) (a) $ABCF$；(b) $ABCEF$；(c) $ABEF$；(d) $ABECF$；(e) $ADEF$；(f) $ADECF$；(g) $ADEBCF$；(h) $ADEBCEF$.

(3) $d(A,F)=3$.

4. (1) v_1 到 v_4 长度为 1 和 2 的路：没有. v_1 到 v_4 长度为 3 的路一条：$v_1v_2v_3v_4$.

(2) v_1 到 v_1 长度为 1 的回路一条：v_1v_1. v_1 到 v_1 长度为 2 的回路一条：$v_1v_1v_1$. v_1 到 v_1 长度为 3 的回路两条：$v_1v_1v_1v_1$，$v_1v_2v_3v_1$.

(3) 图中长度为 3 的路共有 30 条，其中有 4 条回路.

5. 显然，在同一个图 G 中任意两条最长轨迹的长度是相同的. 若图 G 存在两条最长轨迹 L_1：$u_0u_1\cdots u_n$ 和 L_2：$v_0v_1\cdots v_n$ 没有公共节点. 因为 G 的任意两个节点之间都存在一条路，必存在一条最短路径从 L_1 中节点 u_i 到 L_2 中节点 v_j.

(1) 若 $i\leqslant j$，则轨迹 L：$v_0v_1\cdots v_{j-1}v_j\cdots u_iu_{i+1}\cdots u_n$ 的长度大于 n.

(2) 若 $i>j$，则轨迹 L：$u_0u_1\cdots u_{i-1}u_i\cdots v_jv_{j+1}\cdots v_n$ 的长度大于 n.

6. 不妨设 $k=\delta^-$，对于 G 中最长轨迹 L：$u_0\cdots v_0$，若 L 的长度 $<k$，由于 $k=\delta^-$ 且 G 是简单有向图，必存在不在 L 上的节点 w_0 邻接到 u_0，于是 $w_0u_0\cdots v_0$ 是一条比 L 长 1 的轨迹，矛盾.

7. 若 G 中存在节点 u 和 v 有 $\deg^+(u)=\deg^+(v)$. 因为 G 是竞赛图，不妨设 $(u,v)\in$

$E(G)$,由于$\deg^+(u)=\deg^+(v)$,于是在 G 中必存在一个节点 w 使得$(v,w)\in E(G)$而$(u,w)\notin E(G)$. 由$(u,w)\notin E(G)$可得出$(w,u)\in E(G)$,进而 $uvwu$ 为 G 的回路,矛盾.

8. 对于任意 $v_1\in V$,由于 $\deg^-(v_1)\geqslant 2$,必存在 $v_2\in V$ 使得$(v_2,v_1)\in E$. 由于$\deg^-(v_2)\geqslant 2$,必存在 $v_3\in V$ 使得$(v_3,v_2)\in E$. 以此类推,得到轨迹$\cdots v_3v_2v_1$,由于任意节点 $v\in V$ 的入度$\deg^-(v)\geqslant 2$,所以必存在一个圈.

设 m 是满足下列条件的最小下标:(1) $v_m\cdots v_3v_2v_1$ 含有圈 C_1;(2) 对于任意 $k<m$,$v_k\cdots v_3v_2v_1$ 中都不含有圈. 现从 G 中将 C_1 的边全部去掉,得到一个有向图,在该有向图中每节点的入度均$\geqslant 1$,与前面的讨论类似,可得到又一个圈 C_2.

习题 6.5

2. 若 G 不连通,则 G 的连通分支数 $w(G)\geqslant 2$. 任取 G 的 2 个连通分支 C_1 和 C_2,分别在 C_1 和 C_2 中取节点 u 和 v,显然 G 至少有$(1+\deg(u))+(1+\deg(v))\geqslant 2+2\delta(G)\geqslant 2+n$ 个节点,矛盾.

3. 假设 G 不连通,则 G 可以分解成两个不连通的子图 G_1 和 G_2,其阶数分别为 n_1 和 n_2. 由于 $n_1,n_2\geqslant 1$,所以 $n_1,n_2\leqslant n-1$. 又因为 G 是简单图,于是 G_1 和 G_2 是简单图,进而 G_1 的边数$\leqslant n_1(n_1-1)/2$ 且 G_2 的边数$\leqslant n_2(n_2-1)/2$. 而图 G 的边数等于 G_1 与 G_2 的边数之和.

4. 由于 G 不是完全图,必存在 $u,w\in V$ 使得$\{u,w\}\notin E$. 又由于 G 是连通的,u 可达 w,即 u 到 w 存在一条路 L:$uv_0\cdots w$. 对 L 的长度 l 归纳.

若 $l=2$,即 L:uvw,结论成立.

假设 $l=k$ 时结论成立,当 $l=k+1$ 时,分两种情况讨论:

(1) v_0 与 w 邻接,令 $v=v_0$ 结论成立.

(2) v_0 与 w 不邻接,由于 v_0 到 w 存在一条长度为 k 的路 $L-\{u,v_0\}$,取 $u=v_0$,根据归纳假设知结论成立.

5. (1) 对于 G 中最长的路径 L:$v_0v_1\cdots v_l$,其长度为 l,设 G 中与 v_0 邻接的节点有 p 个,因为 $\delta(G)=k$,显然 $p\geqslant k$. 由于 L 是最长路径,于是与 v_0 邻接的 p 个节点必在 L 上,否则会得出一条比 L 更长的路径,不可能. 而这时显然有 $p\leqslant l$,进而 $l\geqslant k$.

(2) 若 $G-\{v_0,v_1,\cdots,v_{k-1}\}$不连通,显然 $v_k,v_{k+1},\cdots,v_l$ 在同一个连通分支中,则可选取另一个连通分支 C. 令 $u_0u_1\cdots u_m$ 是 C 中的最长的路径,类似于(1)的证明,可以得出 C 中与 u_0 邻接的节点个数$\leqslant m$ 且全在 $u_0u_1\cdots u_m$ 路径上. 由于 G 是连通图,G 中与 C 中节点邻接的节点只可能为 $v_0,v_1,\cdots,v_{k-1}$. 分两种情况讨论:

① $v_0,v_1,\cdots,v_{k-1}$中存在节点与 u_0 邻接. 令 v_i 是与 u_0 邻接的下标最小的节点,则路径 $v_lv_{l-1}\cdots v_k\cdots v_{i-1}v_iu_0u_1\cdots u_m$ 的长度为 $l-i+1+m$. 根据 L 是最长路径,知 $l-i+1+m\leqslant l$,于是 $i\geqslant m+1$. 于是 $v_0,v_1,\cdots,v_{k-1}$中至多有 $k-i$ 个节点与 u_0 邻接,进而 $\deg(u_0)\leqslant(k-i)+m\leqslant k-1$,与 $\delta(G)=k$ 矛盾.

② $v_0,v_1,\cdots,v_{k-1}$中不存在节点与 u_0 邻接,这时与 u_0 邻接的节点全在 C 中. 由于 $\delta(G)=k$,因此 $m=k$,即 u_0 与路径 $u_0u_1\cdots u_m$ 上的其余节点均邻接. 因为 C 中必存在节点 u 与 v_0,$v_1,\cdots,v_{k-1}$某节点 v_i 邻接,而 u 可达 $u_0,u_1,\cdots,u_m$ 中任意节点,令 v 是第一个在 C 中与 u_0,$u_1,\cdots,u_m$ 某节点 u_j 邻接而不在 $u_0u_1\cdots u_m$ 上的节点,这时路径 $v_lv_{l-1}\cdots v_kv_{k-1}\cdots v_iu\cdots vu_ju_{j-1}\cdots u_0u_{j+1}\cdots u_m$ 的长度至少为 $l+1$,矛盾.

6. 每个 P 的等价类是无向图 G 的连通分支的节点集合.

7. $\kappa(K_n)=\lambda(K_n)=n-1$.

8. 设 $G=(V,E)$,L:$v_0v_1\cdots v_l$ 是 G 的最长路径,这时与 v_0 以及与 v_l 邻接的节点均在 L 上.

(反证)假设 $l<2\delta(G)$,设与 v_0 邻接的节点分别为 $v_{i_1},v_{i_2},\cdots,v_{i_{1p}}$,而 $v_{i_1-1},v_{i_2-1},\cdots,v_{i_{1p}-1}$与 v_l 不邻接,则 $\deg(v_l)\leqslant l-p$,于是

$$\deg(v_0)+\deg(v_l)\leqslant p+l-p=l<2\delta(G)$$

而 $\deg(v_0)$,$\deg(v_l)\geqslant\delta(G)$,即 $\deg(v_0)+\deg(v_l)\geqslant 2\delta(G)$,矛盾. 于是必存在节点 v_i 与 v_l 邻接且节点 v_{i+1} 与 v_0 邻接,进而得到一条长度为 l 的 G 的最长路径

$$v_{i+2}v_{i+3}\cdots v_lv_i\cdots v_1v_0v_{i+1} \text{ 或 } v_{i-1}v_{i-2}\cdots v_1v_0v_{i+1}\cdots v_lv_i,$$

而路径的起点与终点邻接.

不妨设最长路径 L : $v_0v_1\cdots v_l$ 的起点与终点邻接. 由于路径长度为 $l<2\delta(G)$,而 $|V|>2\delta(G)$,必存在一个节点 u 不在 L 上. 因为 G 是连通图,不妨设 u 与 L 上的节点 v_i 邻接,则路径

$$uv_iv_{i-1}\cdots v_1v_0v_lv_{l-1}\cdots v_{i+1}$$

的长度为 $l+1$,矛盾.

9. 任意删除 G 的 $k-1$ 个节点得到图 G',这时 G' 的阶数为 $n'=n-k+1$,而 $\delta(G')\geqslant(n+k-1)/2-(k-1)=(n-k+1)/2=n'/2$,由第 2 题知 G' 是连通的,故 $\kappa(G)\geqslant k$.

10. $\delta(G)\leqslant 2m/n$.

12. ($\Rightarrow$)(反证)若存在 $\varnothing\neq W\subset V$,而不存在 G 中起点在 W,终点在 $V-W$ 的边,显然 W 中节点不可达 $V-W$ 中节点,这与 G 是强连通图条件矛盾.

($\Leftarrow$)对于任意 $u,v\in V$,由于 G 的边连通度至少为 1,因此 u 到 $V-\{u\}$中节点 u_1 有边,即$(u,u_1)\in E$. 对于 $W=\{u,u_1\}$,必存在节点 $u_2\in V-W$ 使得$(u,u_2)\in E$ 或$(u_1,u_2)\in E$,于是总存在从 u 到 u_2 的路. 继续这个过程,一定存在从 u 到 v 的路.

由于 $u,v\in V$ 的任意性知,G 是强连通图.

习题 6.6

1. (a) $\boldsymbol{A}(G_1)=\begin{bmatrix}1&1&0\\1&0&2\\0&2&0\end{bmatrix}$, $\boldsymbol{P}(G_1)=\begin{bmatrix}1&1&1\\1&1&1\\1&1&1\end{bmatrix}$.

(b) $\boldsymbol{A}(G_2)=\begin{bmatrix}1&1&0\\0&0&0\\0&2&0\end{bmatrix}$, $\boldsymbol{P}(G_2)=\begin{bmatrix}1&1&0\\0&1&0\\0&1&1\end{bmatrix}$.

2. (1) 从 v_3 到 v_2 长度为 4 的路有 2 条,分别为 $v_3v_1v_4v_3v_2$ 和 $v_3v_2v_4v_3v_2$.

(2) G 中长度为 3 的路共有 26 条,其中有 6 条回路.

(3) G 是强连通图.

3. (1) 图 G 的邻接矩阵 $\boldsymbol{A}=\begin{bmatrix}1&2&1&0\\0&0&1&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$.

(2) G 中 v_1 到 v_4 的长度为 4 的路有 4 条，分别为 $v_1e_1v_1e_1v_1e_4v_3e_6v_4$，$v_1e_4v_3e_6v_4e_7v_3e_6v_4$，$v_1e_1v_1e_2v_2e_5v_3e_6v_4$，$v_1e_1v_1e_3v_2e_5v_3e_6v_4$.

(3) G 中 v_1 到 v_1 的长度为 3 的回路有 1 条，它是 $v_1e_1v_1e_1v_1e_1v_1$.

(4) G 中长度为 4 的路共有 16 条，其中有 3 条回路.

(5) G 中长度$\leqslant$4 的路共有 46 条，G 中长度$\leqslant$4 的回路有 8 条.

(6) G 是单向连通图.

4. $\boldsymbol{M}(G_1)=\begin{bmatrix}0&0&0&1&0&1\\2&1&1&0&0&0\\0&1&1&0&1&1\\0&0&0&1&1&0\end{bmatrix}$，$\boldsymbol{M}(G_2)=\begin{bmatrix}-1&0&0&1&0\\1&1&-1&0&0\\0&-1&1&0&1\\0&0&0&-1&-1\end{bmatrix}$

习题 6.7

2. v_4 到 v_1，v_2，v_3 的不存在路径，v_4 到 v_5，v_6，v_7 的最短路径分别为 v_4v_5，$v_4v_5v_6$，$v_4v_5v_6v_7$.

3. 从 u 到 v 的最短路径只有一条 $udecfhv$，其权为 9.

习题 7.1

3. 图 7-3(a)可以. 图 7-3(b)不可以.

4. (1) 4 笔可以画出：aei，kgc，$badcbfjilkj$，$dhefghl$. (2) 两笔可以画出：$eabiadhg$，$fgcjdcbfeh$.

7. 先利用迪杰斯特拉(Dijkstra)算法求出 v_1 到 v_6 的最短路径为 $v_1v_4v_5v_2v_6$，再将该路径所经过的边重复一次即可.

8. 先利用迪杰斯特拉(Dijkstra)算法求出 B 到 E 的最短路径为 BGE，其权为 28，再将该路径所经过的边重复一次即可，于是从邮局 C 出发的一条欧拉回路为 $CBGEGBAFDACDEC$，其权为 281.

10. 对 k 归纳. 当 $k=1$ 时，G 恰含两个度数为奇数的节点，由定理 7-3 知结论成立.

假定$\leqslant k$ 时成立，当连通图有 $2(k+1)$个奇数节点时，任意取 $v_1, v_2\in V$，由于 G 连通，必存在从 v_1 到 v_2 的路径 L，从 G 中删除路径 L 中的所有边，得连通分支 $G_1, G_2, \cdots, G_r$ $(r\geqslant 1)$. 若存在节点度数全为偶数的连通分支，根据欧拉定理，该连通分支中存在欧拉回路，该欧拉回路与路径 L 一起构成一条轨迹. 因此不妨设连通分支 $G_1, G_2, \cdots, G_s$ $(1\leqslant s\leqslant r)$中有度数为奇数的节点，根据握手定理知，度数为奇数的节点个数为偶数 $2k_i$ $(i=1,2,\cdots,s)$. 由于 v_1 和 v_2 的度数为奇数，因此 $\sum_{i=1}^{s} k_i = k$，进而 $k_i\leqslant k$. 根据归纳假设知，对于连通分支 G_i $(i=1,2,\cdots,s)$，G_i 中存在 k_i 条轨迹，它们包含了 G_i 中的所有边. 于是 G 中存在 $\sum_{i=1}^{s} k_i+1=k+1$ 条轨迹，它们包含了 G 中的所有边.

习题 7.2

1. 图 7-14 所示的两个(a)、(b)均是哈密尔顿图.

3. (1) 彼得森图不是哈密尔顿图. (2) 可添加节点 a 与 l 之间的一条边，得到一个哈密尔顿图. (3) 不能. (4) 是.

5. 可以. 将立方体投影在平面上.

6.（1）对于 G 中任意两个不相邻的节点 u 和 v，有 $\deg(u)+\deg(v)\geqslant n$.（2）不一定.

7. 对于任意不相邻的节点 $u,v\in V$，考虑任意节点 $w\in V-\{u,v\}$. 根据已知条件，u 与 w 或 v 与 w 邻接. 又因为 u 与 v 不邻接，因此 u 与 w 且 v 与 w 邻接. 根据 w 的任意性有 $\deg(u),\deg(v)\geqslant n-2$，于是 $\deg(u)+\deg(v)\geqslant 2(n-2)$. 由于 $n\geqslant 4$，所以 $2(n-2)\geqslant n$，于是 $\deg(u)+\deg(v)\geqslant n$.

8. K_n 中有 $\frac{1}{2}(n-1)!$ 条不同的哈密尔顿回路.

10. 哈密尔顿回路在节点 h,j,l 处各只有两条边经过，于是分别有 3 条边不能行遍，共有 9 条边. 哈密尔顿回路在节点 a,c,e 处也各只有两条边经过，各有 1 条边不能行遍，共有 3 条边. 在节点 p 处也只有两条边供行遍. 于是可供行遍的边 $\leqslant 27-(9+3+1)=14$，故所给的图不是哈密尔顿图.

11. 权最小的哈密尔顿回路为 $v_1v_4v_3v_2v_1$.

习题 7.3

1. 所有不同构的 5 阶、6 阶无向树分别有 3 棵和 6 棵.

2.（1）G 有 14 个节点.

3. 叶节点的个数 $x=n_3+2n_4+\cdots+(k-2)n_k+2$.

5. 设 G 是 n 阶无向树，它有 x 片树叶. 若 $x<k$，由于 G 至少有一个节点的度数大于等于 k，则 G 的其余 $n-x-1$ 个节点度数均大于等于 2. 根据握手定理，有

$$2(n-1)=\sum_{i=1}^{n}\deg(v_i)\geqslant 2(n-x-1)+k+x$$

由此可得出 $x\geqslant k$，这与 $x<k$ 矛盾. 所以 G 至少有 k 片树叶.

6. 设 G 是 n 阶无向树，它恰有两片树叶，于是其余 $n-2$ 个节点 $v_1,v_2,\cdots,v_{n-2}$ 中的每个节点至少为 2 度. 根据握手定理，有

$$2(n-1)=2+\sum_{i=1}^{n-2}\deg(v_i)$$

因此对于任意 $i(i=1,2,\cdots,n-2)$，有 $\deg(v_i)=2$. 这时，G 中存在一条从一个叶节点到另一个叶节点的欧拉轨迹，且该轨迹是一条路径.

7. 图 8-4(a)和图 8-4(b)所示的两个图，所有不同构的生成树分别有 3 棵和两棵.

8. K_6 中所有不同构的生成树共 5 棵.

9. 最小生成树的权为 16.

10.（2）对于 n 归纳. 当 $n=2$ 时，显然成立. 假设 $n-1$ 时结论成立，对于 n 个正整数 $(n\geqslant 2)d_1,d_2,\cdots,d_n$，因为 $\sum_{i=1}^{n}d_i=2(n-1)$，所以必存在一个正整数为 1，不妨设 $d_n=1$，同时必存在一个大于等于 2 的正整数，不妨设为 d_{n-1}. 考虑 $n-1$ 个正整数 $d_1,d_2,\cdots,d_{n-2},d_{n-1}-1$，由于 $d_1+d_2+\cdots+d_{n-2}+(d_{n-1}-1)=2[(n-1)-1]$，根据归纳假设知，存在一棵 $n-1$阶无向树，其节点度数分别为 $d_1,d_2,\cdots,d_{n-2},d_{n-1}-1$. 在该树的基础上，增加一个与度数为 $d_{n-1}-1$ 节点邻接的 1 度节点，所得到的 n 阶无向树，其节点度数分别为 $d_1,d_2,\cdots,d_n$.

习题 7.4

2. 所有不同构的 4 阶根树及 5 阶根树分别有 4 棵和 9 棵.

4. (a)、(b)不同构的是根树的生成子图分别有 1 棵和 3 棵.

10. 显然 A_1 和 A_2 的各符号串互不为前缀，因此 A_1 和 A_2 是前缀码. 在 A_3 中 1 既是 11 的前缀，又是 101 的前缀，所以 A_3 不是前缀码.

习题 7.5

2. (1) 若 G 不是连通图，则 G 至少有两个连通分支. 设 C_1 和 C_2 是 G 的两个连通分支，在 C_1 和 C_2 中各取一个节点 u 和 v，于是在 G 添加一条边 uv 所得到的图 $G+uv$ 仍是平面图，这与 G 是极大平面图相矛盾，于是 G 是连通图.

(2) 由于极大平面图是简单图，于是 G 的每个面至少 3 条边围成. 假设存在 G 的 1 个面 R 至少由 4 条边围成，其面的边界为 $v_1v_2v_3v_4\cdots v_1$. 若 v_1 与 v_3 在 G 中不邻接，则在 R 内添加边 v_1v_3，所得到的图仍为平面图，与已知矛盾. 于是 v_1 与 v_3 在 G 中邻接且边 v_1v_3 在 R 的外部. 同样 v_2 与 v_4 在 G 中也邻接且边 v_2v_4 也在 R 的外部. 因此得到两条边 v_1v_3 和 v_2v_4，它们相交于 R 的外部，这与 G 是平面图相矛盾. 故 G 的每个面都是三角形.

3. 不妨设 G 的阶数 $n\geqslant 3$，否则结论是显然的. 根据推论 1 知，$m\leqslant 3n-6$. 若 G 的任意节点 v 的度数均有 $\deg(v)\leqslant 4$，由握手定理知

$$2m=\sum_{v}\deg(v)\geqslant 5n$$

于是 $n\leqslant\frac{2}{5}m$，进而 $m\leqslant 3n-6\leqslant 3\times\frac{2}{5}m-6$. 因此 $m\geqslant 30$，与已知矛盾. 所以问题得证.

4. (反证)假设 G 和 $\overline{G}$ 都是平面图，则根据推论 1 知 G 和 $\overline{G}$ 的边数均小于等于 $3n-6$，其中 n 是 G 或 $\overline{G}$ 的节点数. 由于 G 和 $\overline{G}$ 的边数之和为 K_n 的边数 $\frac{1}{2}n(n-1)$，于是 $\frac{1}{2}n(n-1)\leqslant 2(3n-6)$，即 $n^2-13n+24\leqslant 0$，由此可得 $n<11$，矛盾. 故 G 或 $\overline{G}$ 不是平面图.

5. (反证)假设彼得森图 G 是平面图，由于 G 是连通图，根据欧拉公式，G 的面数为 $m-n+2$. 因为的每个面至少由 5 条边围成，但每一条边是两个面的边界，于是 $5(m-n+2)/2\leqslant m$，所以 $3m-5n+10\leqslant 0$. 因为彼得森图 G 有 $m=15$，$n=10$，于是 $3\cdot 15-5\cdot 10+10=5\leqslant 0$，显然不可能. 因此彼得森图是非平面图.

6. (反证)设 G 是 (n,m) 图，这里 $m=7$. 根据推论 1 知，$m\leqslant 3n-6$，即 $7\leqslant 3n-6$，于是 $3n\geqslant 13$. 根据握手定理，有 $2\times 7=\sum_{v}\deg(v)\geqslant 3n$，即 $3n\leqslant 14$.

9. 由定理 7-11 知，任何简单平面图必存在一个度数小于等于 5 的节点. 不妨假设 G 是连通的，否则 G 至少两个连通分支，若存在一个连通分支其节点个数大于等于 3 或每个连通分支的节点个数均小于等于 2 结论均成立. 当 $n\geqslant 3$ 时，若恰有两个节点度数小于等于 5，则其余 $n-2$ 个节点的度数均大于等于 6，于是 $\sum_{v}\deg(v)\geqslant 6(n-2)+2$. 根据定理 7-11 的推论 1 可知 $m\leqslant 3n-6$，由握手定理有 $\sum_{v}\deg(v)=2m\leqslant 2(3n-6)$. 矛盾.

12. 根据欧拉公式知，面数 $r=m-n+2=12-6+2=8$. 由于每条边恰为两个面的边界，因此围所有面的边数之和为 $2\times 12=24$. 又由于简单平面图的每个面至少 3 条边围成，所以围每个面所需的边数恰为 3.

13. 平面图 G 的对偶图 G^* 是欧拉图的充要条件是 G 的每个面均由偶数条边围成.

14. G 的对偶图 G^* 不是欧拉图，因为 G^* 中无限面所在节点的度数为奇数 7. G^* 也不是哈密尔顿图，因为 G^* 中无限面所在节点为割点.

15. 考虑平面图 G 的对偶图 G^*，由已知条件知 G^* 是无向完全图 K_r. 由于 G^* 是平面图，而 K_r 为平面图时，r 的最大值为 4.

16. 由于极大平面图的每个面都是三角形，因此 G^* 的每个节点的度数为 3，所以 G^* 是 3-正则图. 在 G^* 中任意删除一条边 $e^*=u^*v^*$，则 u^* 和 v^* 所在的两个面是相邻的. 由于 G^* 的每个面都是三角形，于是 G^* 中删除 e^* 后仍存在一条从 u^* 到 v^* 的路，因此仍是连通的，故 G^* 的边连通度 $\lambda(G^*)\geqslant 2$.

17. (1) 根据欧拉公式，有 $r=m-n+2$. 当 $n\geqslant 3$ 时有 $m\leqslant 3n-6$，于是 $r\leqslant(3n-6)-n+2\leqslant 2n-4$.

(2) (反证)设 G 中至多含 5 个节点的度数小于等于 5，则其余 $n-5$ 个节点的度数均大于等于 6. 由于 $\delta(G)=4$，根据握手定理，有

$$5\times 4+6(n-5)\leqslant \sum_v \deg(v)=2m\leqslant 2(3n-6)$$

于是 $6n-10\leqslant 6n-12$，这是不可能的.

18. 不妨设 G 是连通图. 根据欧拉公式，有 $r=m-n+2$. 由握手定理知 $3n\leqslant\sum_v \deg(v)=2m$，进而 $-n\geqslant -2/3m$. 由于 $r<12$，因此

$$m-2/3m+2\leqslant m-n+2<12$$

于是 $m<30$.

若 G 的每个面至少由 5 条边围成，则 $5r\leqslant 2m$，进而 $r\leqslant 2/5m$，于是 $m-2/3m+2\leqslant r=m-n+2\leqslant 2/5m$，因此 $m\geqslant 30$，矛盾.

(2) 正十二面体图 G(参见图 7-9).

习题 7.6

1. 因为 G 中不含有桥，任何一条边都是两个不同面的边界. 对于任意 G 的节点 v，由于 G 的面色数为 2，于是 $\deg(v)$ 为偶数. 根据欧拉定理知 G 是欧拉图.

3. 图 7-50(a)中各节点着色数和边着色数均为 3；图 7-50(b)中各节点着色数和边着色数均为 4.

5. 由于 $\chi(G)=k$，设图 G 用 $1,2,\cdots,k$ 种颜色对节点着色，且分别涂上这 k 种颜色的节点集合分别为 $V_1,V_2,\cdots,V_k$，则对于任意 $i\neq j$，V_i 与 V_j 之间至少存在一条边，否则可以给 V_i 和 V_j 中的节点涂上同一种颜色，这与已知 $\chi(G)=k$ 矛盾. 于是 G 至少有 $k(k-1)/2$ 条边.

6. (反证)若存在节点 $u\in V$ 的度数 $\deg(u)\leqslant k-2$，由于 $\chi(G)=k$，因此 $\chi(G-u)\leqslant k-1$. 由于 $\deg(u)\leqslant k-2$，对 G 中与 u 邻接的节点至多用 $k-2$ 种颜色着色，$k-1$ 种颜色至少还有一种颜色未用，就用这种颜色对节点 u 涂色，其他节点着色与 $G-v$ 相同，于是得出 $\chi(G)\leqslant k-1$，与已知矛盾. 故 G 的最小度 $\delta(G)\geqslant k-1$.

7. 图 G 的节点着色是一张考试安排表，节点着色需要的颜色种数表示不同考试时间的次数. $\chi(G)$表示安排考试时间的最少次数.

习题 7.7

1. 图 7-53(a)为彼得森图，因此它不是二部图，因为存在一个长度为 5 的圈 $abcdea$.

图 7-53(b)所示的图是二部图，其互补节点集为 $V_1=\{a,d,f,h\}$和 $V_2=\{b,c,e,g\}$.

2. 将 6 人作为节点 a,b,c,d,e,f,若两人至少会同一种语言则相应的两节点邻接,得到一个二部图 G,其互补节点集为 $V_1=\{a,e,f\}$和 $V_2=\{b,c,d\}$.

3. 存在完美匹配 M:{Zhang, English}, {Wang, Chinese}, {Li, Math}, {Zhao, Chemistry}, {Sun, Computer}, {Zhou, Physics}.

6. **证** (⇒)设 G 是二部图,其互补节点集合为 V_1 和 V_2,将 V_1 中的节点涂一种颜色,而将 V_2 中的节点涂另一种颜色,则相邻的节点出现不同的颜色. 考虑到 V_1 和 V_2 可能无节点相邻,所以 $\chi(G)\leqslant 2$.

(⇐)设 $\chi(G)\leqslant 2$,若 $\chi(G)=1$,则由于 G 的阶数大于等于 2,所以 G 是零图,显然 G 是二部图. 若 $\chi(G)=2$,即用两种颜色即可对 G 的节点着色,令着第一种颜色的节点组成的集合为 V_1,着第二种颜色的节点组成的集合为 V_2,于是对于任意边 $e=v_1v_2$,由于 v_1 和 v_2 着色不同,所以它们分别属于不同的集合 V_1 和 V_2,即 V_1 和 V_2 是图 G 的互补节点集合,故 G 是二部图.

7. 假设无向树 G 有两个不同的完美匹配 M_1 和 M_2,考虑 $M_1\oplus M_2$. 由于 $M_1\neq M_2$,所以必存在 $M_1\oplus M_2$ 的一个连通分支,其每个节点的度数为 2,进而在 $M_1\oplus M_2$ 存在圈,这与 G 是无向树条件矛盾. 故无向树至多有一个完美匹配.

8. 对于任意 $W\subseteq V$,令 $G-W$ 的所有含奇数个节点的连通分支分别为 $G_1,G_2,\cdots,G_p$,对于任意 $1\leqslant i\leqslant p$,记 q_i 为 G_i 与 W 之间相连的边数. 因为 G 是 k 正则图,于是有 $q_i=\sum_{v\in V(G_i)}\deg(v)-2\mid E(G_i)\mid=k\mid V(G_i)\mid-2\mid E(G_i)\mid$, 即 q_i 与 k 有相同的奇偶性$(1\leqslant i\leqslant p)$.

又因为 G 是 $k-1$ 边连通的,所以 $q_i\geqslant k(1\leqslant i\leqslant p)$. 于是

$$p\leqslant\frac{1}{k}\sum_{i=1}^{p}q_i\leqslant\frac{1}{k}\sum_{v\in W}\deg(v)=\mid W\mid$$

特别地,当 $W=\varnothing$ 时,由于 n 是偶数,这时 $p=0=|W|$,上式仍成立. 根据 Tutte 定理知,G 存在完美匹配.

习题 8.1

1. 7 种.

2. 21168 个.

3. $(n-2)(n-1)!$个.

4. 2880 种.

5. 455 个.

习题 8.2

2. 12 种选球方式,其中包含 1 种每个球都不选的方式.

3. $a_r=\begin{cases}C_{n+r-1}^{r}, & r\text{ 为偶数}\\ 0, & r\text{ 为奇数}\end{cases}$.

4. 38.

5. $a_n=\dfrac{5^n+3^n}{2}$.

习题 8.3

1. 初始条件为 $a_1=1,a_2=2$. 递归关系为 $a_n=a_{n-1}+a_{n-2}(n\geqslant 3)$.

2．初始条件为 $a_1=1, a_2=1$．递归关系为 $a_n=\sum_{k=1}^{n-1}a_k a_{n-k}(n\geqslant 3)$．

3．初始条件为 $a_0=0, a_1=1, a_2=1, a_3=1$．递归关系为 $a_n=a_{n-2}+2a_{n-3}+a_{n-4}(n\geqslant 4)$．

4．$nn!$．

5．$a_n=\sqrt{5\times 2^n-1}$．

6．$a_n=n^2-n+2$．

7．$a_n=\sum_{k=0}^{n}k\cdot\frac{(-2)^{n-k}}{(n-k)!}$．

8．$a_n=2(3^n-2^n)$．

9．$a_n=\frac{1}{52}(42-29n+7n^2)(-1)^n+\frac{5}{13}2^{n-1}$．

10．$a_n=\frac{103}{8}+\frac{13}{2}n+n^2-\frac{41}{3}2^n+\frac{43}{24}5^n$．

11．$a_n=-14\times 3^n+5\times 4^n+(2n+10)2^n$．

12．$f(n)=n(c+b\ln n)$．

参考文献

[1] 何新贵. 模糊知识处理的理论与技术[M].2 版. 北京：国防工业出版社，1998.

[2] ROSEN K H. Discrete Mathematics and Its Applications 7th ed. [s. l.]：McGraw-Hill Companies，Inc.，2012.

[3] 谭浩强. C 语言程序设计[M].2 版. 北京：清华大学出版社，1999.

[4] 王元元，李尚奋. 离散数学[M]. 北京：科学出版社，1994.

[5] 陈建明，曾明，刘国荣. 离散的数学结构[M]. 西安：西安交通大学出版社，2004.

[6] ROBERTS F S，TESMAN B. 应用组合数学. 2 版. 冯速，译. 北京：机械工业出版社，2007.

[7] 王国胤. Rough 集理论与知识获取[M]. 西安：西安交通大学出版社，2001.

[8] 左孝凌，李为鉴，刘永才. 离散数学[M]. 上海：上海科学技术文献出版社，1982.

[9] 屈婉玲，耿素云，张立昂. 离散数学[M]. 北京：清华大学出版社，2005.

[10] 陈莉，刘晓霞. 离散数学[M]. 北京：高等教育出版社，2002.

[11] 刘爱民. 离散数学[M]. 北京：北京邮电大学出版社，2004.

[12] 傅彦，王丽杰，尚明生，等. 离散数学实验与习题解答[M]. 北京：高等教育出版社，2007.

[13] 李盘林，李丽双，李洋，等. 离散数学[M]. 北京：高等教育出版社，1999.

[14] 王元元. 计算机科学中的现代逻辑学[M]. 北京：科学出版社，2001.

[15] 王岚，乐毓俊. 计算机自动推理与智能教学[M]. 北京：北京邮电大学出版社，2005.

[16] 王朝瑞. 图论[M].3 版. 北京：北京理工大学出版社，2001.

[17] 王树禾. 图论[M]. 北京：科学出版社，2004.

[18] 蒋长浩. 图论与网络流[M]. 北京：中国农业出版社，2001.

[19] BOLLOBAS B. 现代图论[M]. 影印版. 北京：科学出版社，2001.

[20] 郑宗汉，郑晓明. 算法设计与分析[M]. 北京：清华大学出版社，2005.

[21] 严蔚敏，吴伟民. 数据结构[M]. 北京：清华大学出版社，1997.

[22] 刘海明，刘洪. 计算机专业研究生入学考试全真题解(1)——数据结构与离散数学分册[M]. 北京：人民邮电出版社，2000.

[23] 卢开澄. 计算机密码学——计算机网络中的数据保密与安全[M]. 2 版. 北京：清华大学出版社，1998.

[24] 傅彦，顾小丰，王庆先，等. 离散数学及其应用[M]. 北京：高等教育出版社，2007.

[25] 屈婉玲，耿素云，张立昂. 离散数学 [M]. 北京：高等教育出版社，2008.

[26] 王元元，张桂芸. 离散数学导论[M]. 北京：科学出版社，2002.

为更好地服务于教学，本书配套提供智能化的数字教学平台——智学苑（www.izhixue.cn），使用清华大学出版社教材的师生可以在全球领先的教学平台上顺利开展教学活动。

为教师提供

- 通过学科知识点体系有机整合的碎片化的多媒体教学资源——教学内容创新；
- 可画重点、做标注、跨终端无缝切换的新一代电子教材——深度学习模式；
- 学生学习情况的自动统计分析数据——个性化教学；
- 作业和习题的自动组卷和自动评判——减轻教学负担；
- 课程、学科论坛上的答疑讨论功能——教学互动；
- 群发通知、催交作业、调整作业时间、查看作业详情、发布学生答案等课程管理功能——课程实践。

为学生提供

- 方便快捷的课程复习功能——及时巩固所学知识；
- 个性化的学习数据统计分析和激励机制——精准的自我评估；
- 智能题库和详细的习题解答——个性化学习的全过程在线辅导；
- 收藏习题功能（错题本）、在线笔记和画重点等功能——高效的考前复习。

我是教师

- 建立属于我的在线课程！

1. 注册教师账号并登录
2. 搜索教材并激活：输入本书附带的教材序列号（见封底）
3. 进入我的智学>我的课程，选择已经激活教材建立在线课程（SPOC校内课或是MOOC公开课）

我是学生

- 加入教材作者建立的MOOC公开课！

1. 注册学生账号并登录
2. 搜索课程：在课程搜索框输入课程编号 GLY-AAA-0094-0001
3. 激活教材：输入本书附带的教材序列号（见封底）
4. 报名课程

- 加入任课教师建立的SPOC校内课！

1. 注册学生账号并登录
2. 搜索课程：在课程搜索框输入课程编号（课程编号请向您的任课教师索取）
3. 激活教材：输入本书附带的教材序列号（见封底）
4. 报名课程：选择班级输入班级报名密码（报名密码请向您的任课教师索取）

建议浏览器：  Google Chrome  Firefox  IE 10.0+

如有疑问，请联系 service@izhixue.cc 或加入清华教学服务群 213172117。